



Installation Guide for Cisco Unity with IBM Lotus Domino (Without Failover)

Release 5.x
Revised May 1, 2008

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-13599-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Installation Guide for Cisco Unity Release 5.x with IBM Lotus Domino (Without Failover)
© 2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface vii

- Audience and Use vii
- Documentation Conventions vii
- Cisco Unity Documentation xi
- Obtaining Documentation, Obtaining Support, and Security Guidelines xi

CHAPTER 1

Overview of Mandatory Tasks for Installing Cisco Unity 1-1

- Part 1: Installing and Configuring the Cisco Unity Server 1-1
- Part 2: Installing and Configuring a Voice-Recognition Server 1-3
- Part 3: Populating the Cisco Unity System with Subscriber and Call Management Data 1-3
- Part 4: Setting Up Networking Options (If Applicable) 1-4
- Part 5: Customizing the Cisco Unity Conversation 1-5
- Part 6: Backing Up Cisco Unity 1-5
- Part 7: Training 1-5

CHAPTER 2

Preparing for the Installation 2-1

- Gathering Documentation and Tools 2-1
- Downloading Software for the Installation 2-2
- Determining the Locations for Files on the Cisco Unity Server 2-4
 - Locations for Files on a Platform Overlay 1 or Overlay 2 Server 2-4
 - Locations for Files on a Platform Overlay 3 Server 2-5

CHAPTER 3

Setting Up the Hardware 3-1

- Installing Voice Cards 3-1
- Attaching Peripheral Devices and Making Connections from the Phone System 3-4

CHAPTER 4

Installing the Operating System 4-1

- Considerations for Installing Windows 4-2
 - Windows Server 2003 Considerations 4-2
 - Windows 2000 Server Considerations 4-2
 - Additional Considerations for Both Windows Versions 4-2
- Configuring the RAID Arrays (Selected Installations) 4-3

Installing Windows Server 2003 by Using the Cisco Unity Platform Configuration Discs	4-4
Installing Windows 2000 Server by Using the Cisco Unity Platform Configuration Discs	4-6
Installing Windows Server 2003 by Using a Retail Windows Server 2003 Disc	4-8
Installing Windows 2000 Server by Using a Retail Windows Server 2000 Disc	4-9
Creating the Partitions	4-11
Adding 3GB and userva Switches to the Boot.ini File	4-12

CHAPTER 5

Customizing the Cisco Unity Platform 5-1

Configuring a Dual NIC in the Cisco Unity Server	5-2
Installing the NIC-Configuration Utility	5-3
Configuring a Dual NIC	5-4
Obtaining Cisco Unity License Files	5-4
Running the Cisco Unity System Preparation Assistant	5-6
Installing Administration Software for MSDE 2000 and Setting the MSDE System Administrator Password	5-9
Changing Folder Settings in Windows Explorer	5-10
Installing Microsoft Updates and Cisco Security Agent for Cisco Unity	5-10
Disabling the Found New Hardware Wizard for the Voice Cards	5-11
Installing Antivirus Software (Optional)	5-12
Connecting the Cisco Unity Server to the Network	5-12
Configuring TCP/IP Properties	5-12
Verifying the IP Address and the Network Connection	5-13
Disabling Antivirus and Cisco Security Agent Services	5-14
Installing Active Directory or Adding the Cisco Unity Server to an Existing Domain	5-15
Active Directory	5-15
Existing Domain	5-16

CHAPTER 6

Setting Up Domino and Installing Lotus Notes 6-1

Preparing the Domino Server(s) for Cisco Unity	6-1
Installing and Configuring Lotus Notes on the Cisco Unity Server	6-4

CHAPTER 7

Creating Accounts for the Installation and Granting Permissions 7-1

About the Accounts Required for the Cisco Unity Installation	7-1
The Account Used to Install Cisco Unity	7-2
The Account Used to Access the Cisco Unity Administrator	7-2
The Accounts That Cisco Unity Services Log On As	7-2
Creating the Accounts Required for the Cisco Unity Installation	7-2

- Adding the Cisco Unity Administration Account to an Admins Group 7-3
- Granting Permissions with the Cisco Unity Permissions Wizard 7-4

CHAPTER 8

- Installing and Configuring Cisco Unity Software 8-1**
 - Determining Whether to Set Up Cisco Unity to Use SSL 8-2
 - Installing the Microsoft Certificate Services Component 8-2
 - Installing and Configuring Cisco Unity Software 8-3
 - Starting the Cisco Unity Installation and Configuration Assistant and Installing Cisco Unity Software 8-3
 - Installing License Files 8-6
 - Configuring Services 8-7
 - Configuring Cisco Unity for the Message Store 8-7
 - Setting New Default Passwords 8-8
 - Integrating the Phone System with Cisco Unity 8-8
 - Setting Up the Cisco Personal Communications Assistant to Use SSL 8-9
 - Testing the Phone System Integration 8-14
 - Excluding Selected Directories from Virus Scanning 8-14
 - Deleting Apache Tomcat Sample Directories 8-14
 - Setting Up the Cisco Unity Administrator and Status Monitor to Use SSL 8-15
 - Configuring Internet Explorer to Display the Cisco Unity Administrator Correctly (Windows Server 2003 Only) 8-17
 - Securing the Example Administrator Account Against Toll Fraud 8-18
 - Moving the Data Store Databases and Transaction Logs 8-19
 - Installing the Latest Microsoft Service Packs and Updates 8-21
 - Re-enabling Virus-Scanning and Cisco Security Agent Services 8-22
 - Enabling the Unity Messaging Repository Conversation 8-22
 - Securing Cisco Unity and the Cisco Unity Server 8-23

CHAPTER 9

- Installing Optional Software 9-1**
 - Installing Monitoring Software 9-1
 - Installing RSA SecurID 9-1
 - Installing Other Optional Software 9-2

CHAPTER 10

- Setting Up Authentication for the Cisco Unity Administrator 10-1**
 - Determining the Authentication Method to Use for the Cisco Unity Administrator 10-1
 - Authentication Methods Available for the Cisco Unity Administrator 10-2
 - How Integrated Windows Authentication Works with the Cisco Unity Administrator 10-3

How Anonymous Authentication Works with the Cisco Unity Administrator 10-4
 Configuring IIS So That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication 10-6

APPENDIX A

Voice Cards and PIMG Units A-1

Intel Dialogic D/41EPCI, D/41JCT-LS, and D/41JCT-Euro A-1
 Hardware Settings A-2
 Intel Dialogic D/120JCT-LS and D/120JCT-Euro A-4
 Hardware Settings A-6
 Software Settings A-7
 Intel Dialogic D/240PCI-T1 A-8
 Hardware Settings A-9
 Software Settings A-10
 Intel NetStructure PBX-IP Media Gateway (PIMG) A-11
 Software Settings A-12

APPENDIX B

Exiting and Starting the Cisco Unity Software and Server B-1

Exiting the Cisco Unity Software B-1
 Shutting Down or Restarting the Cisco Unity Server B-3
 Starting the Cisco Unity Software B-3

APPENDIX C

Installing and Configuring a Voice-Recognition Server C-1

Creating the Partition C-2
 Installing the Required Windows Server 2003 Service Pack and Updates, and Cisco Security Agent for Cisco Unity C-3
 Adding the Voice-Recognition Server to a Domain (Optional) C-4
 Installing Cisco Unity Voice-Recognition Software C-5
 Configuring Voice-Recognition Software C-5
 Excluding Selected Directories from Virus Scanning C-6
 Installing the Latest Windows Server 2003 Service Pack and Updates C-7

INDEX



Preface

This preface contains the following sections:

- [Audience and Use, page vii](#)
- [Documentation Conventions, page vii](#)
- [Cisco Unity Documentation, page xi](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page xi](#)

Audience and Use

The Cisco Unity installation guide is intended for installers of a Cisco Unity system. You need a working knowledge of IBM Lotus Domino and Microsoft Windows 2003 or Windows 2000, depending on the version you plan to install on the Cisco Unity server.

Documentation Conventions

Table 1 *Cisco Unity installation guide Conventions*

Convention	Description
boldfaced text	Boldfaced text is used for: <ul style="list-style-type: none">• Key and button names. (Example: Click OK.)• Information that you enter. (Example: Enter Administrator in the User Name box.)
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In the Command Prompt window, enter ping <IP address> .)
- (hyphen)	Hyphens separate keys that must be pressed simultaneously. (Example: Press Ctrl-Alt-Delete .)
> (right angle bracket)	A right angle bracket is used to separate selections that you make: <ul style="list-style-type: none">• On menus. (Example: On the Windows Start menu, click Settings > Control Panel > Phone and Modem Options.)• In the navigation bar of the Cisco Unity Administrator. (Example: Go to the System > Configuration > Settings page.)

The Cisco Unity installation guide also uses the following conventions:

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Warning****IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS**Waarschuwing****BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES**Varoitus****TÄRKEITÄ TURVALLISUUSOHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET**Attention****IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung WICHTIGE SICHERHEITSHINWEISE

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza IMPORTANTI ISTRUZIONI SULLA SICUREZZA

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel VIKTIGE SIKKERHETSINSTRUKSJONER

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso INSTRUÇÕES IMPORTANTES DE SEGURANÇA

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! INSTRUCCIONES IMPORTANTES DE SEGURIDAD

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning! VIKTIGA SÄKERHETSANVISNINGAR

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR**Figyelem****FONTOS BIZTONSÁGI ELOÍRÁSOK**

Ez a figyelmeztető jel veszélyre utal. Sérülésveszélyt rejtő helyzetben van. Mielőtt bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplő figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján kereshető meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!**Предупреждение****ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ**警告****重要的安全性说明**

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告**安全上の重要な注意事項**

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

Cisco Unity Documentation

For descriptions and URLs of Cisco Unity documentation on Cisco.com, refer to the *Documentation Guide for Cisco Unity*. The document is shipped with Cisco Unity and is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_documentation_roadmaps_list.html.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>



CHAPTER 1

Overview of Mandatory Tasks for Installing Cisco Unity



Note

If you are upgrading Cisco Unity, refer instead to the *Reconfiguration and Upgrade Guide for Cisco Unity* for upgrade instructions.

Use the following high-level task list to install the Cisco Unity system correctly. The tasks reference detailed instructions in the Cisco Unity installation guide, and in other Cisco Unity documentation as noted. Follow the documentation for a successful installation.

The task list leads you through the complete installation of the Cisco Unity system—from installing and configuring the Cisco Unity server; to populating the Cisco Unity system with subscriber and call management data; to setting up optional features, such as networking; to backing up Cisco Unity.



Note

Cisco assumes that the Domino environment is already set up and working before the Cisco Unity system is installed.

The list is divided into seven parts. Some of the tasks apply only to specific situations, and are noted as such. If a task does not apply to your situation, skip it.

Part 1: Installing and Configuring the Cisco Unity Server

The tasks in Part 1 reference chapters in the Cisco Unity installation guide, unless otherwise noted.

1. Confirm that you are using the correct version of the Cisco Unity installation guide for your configuration. This version of the guide is for Cisco Unity 5.0(1) and later Unified Messaging with Domino (without Cisco Unity failover). For a list of configurations and applicable installation guides, refer to the document *Use the Installation Guide That Matches the Cisco Unity 5.x Configuration* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.
2. Verify the following requirements:
 - a. System requirements for the Cisco Unity 5.x system. Refer to the applicable version of *System Requirements for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

- b. Requirements for integrating the phone system(s). Refer to the “Requirements” section of the applicable Cisco Unity integration guide(s) at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.
 - c. *If the system is using Cisco Unity Bridge Networking*: Requirements for the Bridge. Refer to the applicable version of *System Requirements, and Supported Hardware and Software for Cisco Unity Bridge* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.
 - d. *If the system is using any Cisco Unity networking option (including the Bridge)*: Requirements for the networking option. Refer to *Networking Options Requirements for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.
3. Gather the documentation and tools for the installation, download the latest Cisco Unity Server Updates wizard and other software, and determine the drive locations for application, log, and database files that you will need later in the installation. See [Chapter 2, “Preparing for the Installation.”](#)
4. Set up or program the phone system(s) and extensions to enable the integration(s) with Cisco Unity. Refer to the “Programming the <Name> Phone System” section of the applicable Cisco Unity integration guide(s) at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.
5. Install voice cards in the Cisco Unity server or an expansion chassis; set up the server and attach peripheral devices, if applicable; and make connections from the phone system. See [Chapter 3, “Setting Up the Hardware.”](#)
6. Configure the RAID arrays, if applicable, install Windows Server 2003 or Windows 2000 Server, and create the partitions, if applicable. See [Chapter 4, “Installing the Operating System.”](#)
7. Obtain Cisco Unity license files, and use the Cisco Unity System Preparation Assistant to configure the operating system and install required software components. Then set up the server in the Windows networking environment. See [Chapter 5, “Customizing the Cisco Unity Platform.”](#)
8. Prepare the Domino server for Cisco Unity, and install and configure Lotus Notes on the Cisco Unity server. See [Chapter 6, “Setting Up Domino and Installing Lotus Notes.”](#)
9. Create the accounts required for the Cisco Unity installation, and set rights and permissions. See [Chapter 7, “Creating Accounts for the Installation and Granting Permissions.”](#)
10. Decide whether to set up Cisco Unity to use SSL and install the Microsoft Certificate Services component, if applicable, then use the Cisco Unity Installation and Configuration Assistant to install and configure Cisco Unity software, and to set up the Cisco Personal Communications Assistant to use SSL, if applicable. You also set up the Cisco Unity Administrator and the Status Monitor to use SSL, if applicable, then secure the Example Administrator account against toll fraud, and move SQL Server or MSDE database files and transaction logs, if applicable. See [Chapter 8, “Installing and Configuring Cisco Unity Software.”](#)
11. Install any optional software. See [Chapter 9, “Installing Optional Software.”](#)
12. Determine the authentication method that you want to use for the Cisco Unity Administrator web application, and configure IIS, as applicable. See [Chapter 10, “Setting Up Authentication for the Cisco Unity Administrator.”](#)
13. Store all of the software that was shipped with Cisco Unity together in a location that is safe and can be readily accessed. You may need the discs later to upgrade or to otherwise modify the Cisco Unity system, or Cisco TAC may require you to access them during a service call.

Part 2: Installing and Configuring a Voice-Recognition Server

14. Install and configure a voice-recognition server, if applicable. See [Appendix C, “Installing and Configuring a Voice-Recognition Server.”](#)

Part 3: Populating the Cisco Unity System with Subscriber and Call Management Data

You do most of the tasks in Part 3 by using the Cisco Unity Administrator. (For information on logging on to the Cisco Unity Administrator and on using it, refer to the “Accessing and Using the Cisco Unity Administrator” chapter of the *System Administration Guide for Cisco Unity*.)

The tasks reference chapters in the *System Administration Guide for Cisco Unity Release 5.x* that contain detailed information; the guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

15. Define system schedules:
 - a. Identify standard business hours.
 - b. Identify closed and weekend hours.
 - c. Create custom schedules, if necessary.
 - d. Identify holidays.

Refer to the “Creating and Modifying Schedules” and “Identifying Days as Holidays” sections in the “Call Management Overview” chapter.

16. Set up phone, GUI, and TTS languages (including TTY, if applicable). Refer to the “Managing Languages” chapter.
17. Set up third-party fax, if applicable.
18. Create a call management plan. Refer to the “Creating and Implementing a Call Management Plan” section in the “Call Management Overview” chapter.
19. Prepare to create regular subscriber accounts. Refer to the “Issues to Consider Before Creating Regular Subscriber Accounts” section in the “Managing Subscriber Accounts” chapter.
 - a. Confirm that you have the necessary permissions for creating subscriber accounts and that Cisco Unity is configured properly to work with the message store.
 - b. Confirm that you have the applicable licenses.
 - c. Determine password and account lockout policy for Cisco Unity phone access.
 - d. Determine logon, password, and account lockout policy for Cisco Unity web access.
 - e. Decide whether to set up enhanced phone security.
 - f. Review, change, and create classes of service.
 - g. Create restriction tables, and assign them to the appropriate class(es) of service.
 - h. Create public distribution lists.
 - i. Review, create, and modify subscriber templates. Secure phone passwords.
 - j. Confirm that the address book(s) listed on the System > Configuration > Subscriber Address Books page in the Cisco Unity Administrator contain the user data that you want to import when you create subscriber accounts.

20. Test the system configuration:
 - a. Add a single subscriber (refer to the “Managing Subscriber Accounts” chapter). After you create the subscriber account, the Domino server needs additional time to enable IBM Lotus Domino Unified Communications (DUC) for Cisco for the user. Wait several minutes before proceeding with Task b.
 - b. Use the phone to log on to Cisco Unity as the test subscriber, record a name, and set a phone password. Hang up.
 - c. Call Cisco Unity and log on as the test subscriber again to confirm that the password, greeting, and conversation specified for the subscriber are working properly. Confirm that the subscriber inherited the correct class of service by testing any applicable features by phone. (If the Cisco Unity conversation indicates that messages are not yet available, it may be that the Domino server has not finished enabling the subscriber account to use DUC for Cisco. Wait a few more minutes, and try again.)
 - d. Log on to the Cisco Personal Communications Assistant (PCA) as the test subscriber. If you gave the test subscriber the required class of service rights, test to see if you can browse from the Cisco PCA Welcome page to the Cisco Unity Assistant.
 - e. Make corrections to the system configuration as necessary.
21. Create subscriber accounts. Refer to the “Managing Subscriber Accounts” chapter.
22. Modify individual subscriber accounts as needed. Refer to the “Modifying Subscriber Accounts” section in the “Managing Subscriber Accounts” chapter.
23. Add individual subscribers to public distribution lists, as needed. (For example, assign subscribers to screen those messages left in Cisco Unity that are not associated with a specific recipient, such as those left to the Unaddressed Messages distribution list or for the Opening Greeting call handler.) Refer to the “About Message Handling” section in the “Messaging and Default Accounts Overview” chapter.
24. Implement, then test the call management plan you created in Task 18.:
 - a. Create call handlers. Refer to the “Managing Call Handlers” chapter.
 - b. Specify directory handler settings. Refer to the “Managing Directory Handlers” chapter.
 - c. Create interview handlers. Refer to the “Managing Interview Handlers” chapter.
 - d. Set up call routing. Refer to the “Creating and Modifying Call Routing Rules” section in the “Call Management Overview” chapter.
25. As applicable, set up subscriber phones to access Cisco Unity, and set up Cisco Unity features that subscribers will use, such as IBM Lotus Notes with DUC for Cisco, text-message notifications, and Message Monitor. Refer to the “Setting Up Subscriber Workstations” chapter.

Part 4: Setting Up Networking Options (If Applicable)

26. *If the system is using Digital Networking:* Set up Digital Networking. Refer to the “Digital Networking” chapter of the *Networking Guide for Cisco Unity Release 5.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.
27. *If the system is using Internet Subscribers:* Set up Internet subscribers. Refer to the “Internet Subscribers” chapter of the *Networking Guide for Cisco Unity Release 5.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

28. *If the system is using AMIS Networking:* Set up AMIS Networking. Refer to the “AMIS Networking” chapter of the *Networking Guide for Cisco Unity Release 5.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.
29. *If the system is using VPIM Networking:* Set up VPIM Networking. Refer to the “VPIM Networking” chapter of the *Networking Guide for Cisco Unity Release 5.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.
30. *If the system is using Bridge Networking:* Install the Cisco Unity Bridge server. Refer to the “Overview of Mandatory Tasks for Installing the Cisco Unity Bridge” chapter of the applicable *Installation Guide for Cisco Unity Bridge* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.
31. *If the system is using Bridge Networking:* Set up Cisco Unity and the Bridge for networking. Refer to the “Setting Up Cisco Unity and the Bridge for Networking” chapter of the applicable *Networking Guide for Cisco Unity Bridge* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

Part 5: Customizing the Cisco Unity Conversation

32. When callers access Cisco Unity by phone, they hear a set of prerecorded instructions and options known as the Cisco Unity conversation (also known as the TUI, or telephone user interface). You can customize the conversations that subscribers and unidentified callers hear in several ways.

For example, you may want to change how Cisco Unity handles messages that are interrupted by disconnected calls, specify that Cisco Unity prompts subscribers to record first and then address when they send messages, offer “Easy” Sign-In and system transfers, or specify that Cisco Unity plays additional caller information when subscribers play messages.

You may also want to set up the Cisco Unity Greetings Administrator or the Cisco Unity Broadcast Message Administrator for system administrators to use.

Refer to the “Cisco Unity Conversation Overview” chapter of the *System Administration Guide for Cisco Unity Release 5.x* at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html for details on these and other conversation customizations.

Part 6: Backing Up Cisco Unity

33. Back up Cisco Unity. Refer to the “About Backing Up a Cisco Unity System” chapter of the *Maintenance Guide for Cisco Unity Release 5.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Part 7: Training

34. Train subscribers, operators, and support desk personnel to use Cisco Unity. Refer to the “Subscriber Orientation” chapter of the *System Administration Guide for Cisco Unity Release 5.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.



CHAPTER 2

Preparing for the Installation

In this chapter, you do the following tasks in the order listed:

1. Gather the documentation and tools needed for the installation. See the “[Gathering Documentation and Tools](#)” section on page 2-1.
2. Download the software needed for the installation. See the “[Downloading Software for the Installation](#)” section on page 2-2.
3. Determine and record the file locations for application, log, and database files on the Cisco Unity system. See the “[Determining the Locations for Files on the Cisco Unity Server](#)” section on page 2-4.

When you are finished with this chapter, return to [Chapter 1, “Overview of Mandatory Tasks for Installing Cisco Unity”](#) to continue installing the Cisco Unity system correctly:



Note

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Gathering Documentation and Tools

You need the following items during the installation and configuration of the Cisco Unity system:

- Access to the following Cisco Unity documentation.
 - Release notes for the applicable version of Cisco Unity.
 - Release notes for the applicable version of Cisco Security Agent for Cisco Unity, if applicable.
 - The correct version of the Cisco Unity installation guide for your configuration. (Refer to the document *Use the Installation Guide That Matches the Cisco Unity 5.x Configuration* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.)
 - The *Documentation Addendum for Cisco Unity* for the applicable version of Cisco Unity (for versions 5.1 and later).
 - Specifications for the server on which you are installing Cisco Unity. (Refer to the *Cisco Unity Supported Platforms List* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.)
 - The Cisco Unity integration guide(s) for your phone system(s).

- If you are integrating Cisco Unity with Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager), release notes for the applicable version of the Cisco Unity-CM TSP.
- The *System Administration Guide for Cisco Unity*.
- If you are setting up Cisco Unity Digital Networking, AMIS or VPIM networking, or Internet subscribers, the *Networking Guide for Cisco Unity*.
- If you are setting up Bridge Networking, release notes for the applicable version of the Cisco Unity Bridge, the *Installation Guide for Cisco Unity Bridge*, and the *Networking Guide for Cisco Unity Bridge*. Also, release notes for the applicable version of Cisco Security Agent for Cisco Unity Bridge, if applicable.

Cisco Unity documentation is available at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html.

- Two test phones.

Downloading Software for the Installation

Revised May 1, 2008

This section lists the software needed to install Cisco Unity. If your Cisco Unity DVDs are an earlier version than the currently shipping version, download all of the software listed in this section.

Note the following considerations:

- The downloads may total several GB. Use a computer with a high-speed Internet connection, and confirm that the computer has sufficient disk space or has access to a network drive with sufficient disk space.
- Most downloads are self-extracting executable files. When downloads are complete, extract the updates and burn DVDs that contain the extracted files. Then delete the downloaded .exe files to free disk space.

For detailed instructions on downloading software and burning DVDs, refer to the “Installation and Upgrade Information” section of the applicable release notes, available at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.



Caution

Until you have installed all of the recommended service packs and updates, and, optionally, Cisco Security Agent for Cisco Unity and antivirus software, third-party components installed on the Cisco Unity server have significant security vulnerabilities. Do not connect the Cisco Unity server to the network to install software. Instead, burn DVDs that contain the downloaded software, and install the software from the DVDs.

- The Cisco Unity documentation instructs you when to install the software you download.



Note

To access the software download page, you must be logged on to Cisco.com as a registered user.

Download the following software for all installations. Even if you have Cisco Unity DVDs for the currently shipping version, we recommend that you download the software, some of which may have been released or updated after the discs were produced.

Cisco Unity Software

Disc images for the currently shipping Cisco Unity version, including:

- The Cisco Unity installation disc.
- The discs for Cisco Unity languages that you want to install on the server (other than U.S. English, which is automatically installed on all systems).
- The applicable Cisco Unity Service Pack discs for the version of Cisco Unity that you are installing. You always need Service Pack disc 1, which contains the Cisco Unity System Preparation Assistant.

Before you install Cisco Unity, you must install the Microsoft service packs that were required for that version of Cisco Unity. After you install Cisco Unity, you can install any later service packs that were qualified for use with Cisco Unity.

Refer to the “Downloading Software for Cisco Unity <Version>” section of the applicable *Release Notes for Cisco Unity* at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Updated PBXLink or PIMG Firmware

If the phone system integration includes PBXLink boxes or PIMG units, updated PBXLink or PIMG firmware. For instructions on downloading updated firmware, refer to the “Setting Up the PBXLink Box” section or the “Setting up the PIMG Units” section in the applicable Cisco Unity integration guide. Integration guides are available at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

Latest Microsoft Service Packs and Cisco Unity Server Updates Wizard

Download the following software:

- For the Microsoft software that you are installing on the Cisco Unity server, the latest service packs recommended for use with Cisco Unity, if later than the service packs shipped with Cisco Unity. Any service packs that are qualified for use with Cisco Unity after the most recent Cisco Unity release are available on the Microsoft Updates Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity_msft_updates. Also download or print the installation instructions.

For a list of the service packs that are recommended, refer to the section “Recommended Service Packs—Cisco Unity Server” in the *System Requirements for Cisco Unity* for your version of Cisco Unity, at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

- The latest Cisco Unity Server Updates Wizard, which automatically installs the latest Microsoft updates for Windows and for SQL Server or MSDE that are recommended for use with Cisco Unity and, optionally, the latest version of the Cisco Security Agent for Cisco Unity. Available on the Microsoft Updates for Cisco Unity Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity_msft_updates.

For information on the Microsoft updates and the version of Cisco Security Agent for Cisco Unity that are installed by the Server Updates Wizard, refer to *Software Installed by the Cisco Unity Server Updates Wizard* at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Determining the Locations for Files on the Cisco Unity Server

The platform overlay and RAID configuration of the Cisco Unity server determines the choices you make later in the Cisco Unity installation guide, including:

- How you manually configure partitions if you are installing Windows using a retail Windows disc. (If you install Windows using the Cisco Unity Platform Configuration discs, partitions are configured automatically.)
- Where you choose to install applications, logs, and database files.

Using the applicable section, make note of the locations for files on the Cisco Unity server that you are installing:

- [Locations for Files on a Platform Overlay 1 or Overlay 2 Server, page 2-4](#)
- [Locations for Files on a Platform Overlay 3 Server, page 2-5](#)

Following these recommendations will:

- Maximize performance, data integrity, and reliability for Cisco Unity, and SQL Server or MSDE transaction logs.
- Maximize performance, data storage, and access capacity for Cisco Unity data.

For information on the platform overlay, RAID configuration, maximum number of Cisco Unity subscribers, and other specifications for the server on which you are installing Cisco Unity, refer to the *Cisco Unity Supported Platforms List* at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.

The Cisco Unity installation guide alerts you when to refer to the file locations later in the installation process.

Locations for Files on a Platform Overlay 1 or Overlay 2 Server

Table 2-1 lists the file locations for Cisco Unity Platform Overlay 1 servers.



Note

Except for the system partition, drive C:, different letters may be used to label the partitions.

Table 2-1 Locations for Files on a Platform Overlay 1 or Overlay 2 Server

Partition	Files
C	<ul style="list-style-type: none"> • Operating system • Pagefile • For systems up to 32 ports: MSDE 2000 program files (The default partition for MSDE 2000 program files is drive C: and cannot be changed.)
D	<ul style="list-style-type: none"> • SQL Server 2000 or MSDE 2000 databases • SQL Server 2000 or MSDE 2000 transaction logs • Unity Message Repository (UMR) • Program files, including Cisco Unity and Notes and, for systems over 32 ports, SQL Server 2000 • Cisco Unity trace logs

Locations for Files on a Platform Overlay 3 Server

Table 2-2 lists the locations for Cisco Unity Platform Overlay 3 servers.

**Note**

Except for the system partition, drive C:, different letters may be used to label the partitions.

Table 2-2 *Locations for Files on a Platform Overlay 3 Server*

Disk Array	Partition	Files
First	C	<ul style="list-style-type: none">• Operating system• Pagefile
First	D	<ul style="list-style-type: none">• Program files, including Cisco Unity and SQL Server 2000• Cisco Unity trace logs• SQL Server transaction logs
Second	E	<ul style="list-style-type: none">• SQL Server 2000 databases• Unity Message Repository (UMR)



CHAPTER 3

Setting Up the Hardware

In this chapter, you do the following tasks in the order listed:

1. *If the Cisco Unity system is using voice cards to integrate with a circuit-switched phone system:* Install voice cards. See the [“Installing Voice Cards”](#) section on page 3-1.
2. Set up the Cisco Unity server. See the [“Attaching Peripheral Devices and Making Connections from the Phone System”](#) section on page 3-4.

When you are finished with this chapter, return to [Chapter 1, “Overview of Mandatory Tasks for Installing Cisco Unity,”](#) to continue installing the Cisco Unity system correctly.



Note

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Installing Voice Cards



Note

If the system is not using voice cards to integrate with a circuit-switched phone system, skip this section.

All voice cards must be installed in the same server or in the same expansion chassis. If all voice cards do not fit in the Cisco Unity server, then you must install all of them in an expansion chassis.

All Cisco Unity-compatible voice cards are 33-MHz PCI cards. Universal PCI (uPCI) cards work in either 5-Vdc or 3.3-Vdc PCI and PCI-X slots, while non-universal PCI cards work only in 33-MHz (5-Vdc) slots.

If you are installing a uPCI voice card, you can generally place the card in any physically compatible slot in the server or expansion chassis. However, if the slot you choose is a 3.3-Vdc PCI or PCI-X slot (designed to be 66 MHz or faster), that slot and the slot adjacent to it on the same logical PCI bus segment will slow down to 33 MHz to accommodate the 33-MHz card. (For example, if a 33-MHz voice card is placed in a PCI-X slot next to a 133-MHz RAID controller and they share the same logical segment, the RAID controller speed is reduced to 33 MHz.)

Refer to the manufacturer documentation for detailed PCI bus topology information before deciding final slot placement of 3.3-Vdc or 5-Vdc, 33-MHz voice cards.

Note that if you view a voice card by using Windows Device Manager, the card may be displayed as an unknown PCI device, with a warning stating that the drivers for the device are not installed. A Found New Hardware wizard may also appear for each card during installation or when the Cisco Unity server is restarted. These conditions are both expected behavior, and do not indicate an error or a condition

requiring action. You can disable the Found New Hardware wizard to prevent it from appearing when the Cisco Unity server is restarted. The Cisco Unity installation guide alerts you when to do the procedure later in the installation process (“[Disabling the Found New Hardware Wizard for the Voice Cards](#)” section on page 5-11).



Warning

This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.

Statement 1017



Warning

Read the installation instructions before connecting the system to the power source. Statement 1004



Warning

Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.

Statement 1



Warning

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. Statement 1024



Warning

There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions. Statement 1015



Warning

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- **This unit should be mounted at the bottom of the rack if it is the only unit in the rack.**
- **When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.**
- **If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.** Statement 1006



Warning

Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages. Statement 2



Warning

Do not work on the system or connect or disconnect cables during periods of lightning activity.

Statement 1001



Warning

To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord. Statement 1023

**Warning**

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
Statement 1030

**Warning**

This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel. Statement 88

**Warning**

The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards. Statement 117

**Warning**

Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.
Statement 1029

To Install Voice Cards in the Cisco Unity Server or in an Expansion Chassis

- Step 1** If the server is on, shut it down.
- Step 2** Unplug the power cord.
- Step 3** Attach an antistatic wrist strap, and ground yourself to the server.

**Warning**

During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.
Statement 94

- Step 4** Set the switches and jumpers on each card. See the “Hardware Settings” section for your cards in [Appendix A, “Voice Cards and PIMG Units.”](#)
- Some cards include hardware settings that indicate which card is first, which is second, and so on. If you are installing more than one card of the same model, keep the cards in order so you can install them in the correct order in [Step 6](#).
- If you are installing Intel Dialogic D/120JCT-Euro or D/240PCI-T1 cards, do not do the procedure in the “Software Settings” section for your cards in [Appendix A, “Voice Cards and PIMG Units,”](#) at this time. The Cisco Unity installation guide alerts you when to do the procedure later in the installation process.
- Step 5** If you are not using a PCI expansion chassis, skip to [Step 6](#).
- If you are using a PCI expansion chassis, install the host card in a PCI slot that can be used for the host card. For information on which servers support using an expansion chassis and on which slots in those servers can be used for expansion chassis host cards, see the *Cisco Unity Supported Platforms List* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.
- Note the following:

- If the slot location of a customer-provided server management card (such as Hewlett-Packard Remote Insight Lights-Out Edition) conflicts with a required host card slot, the host card takes precedence.
- Using an unapproved slot for the host card can cause a conflict with the RAID controller card.

Step 6 Insert each voice card firmly into its slot in the server or in the expansion chassis, and fasten each card to the back plate with a screw. Note the following considerations, as applicable:

- If you are installing more than one voice card of the same model, and if the cards include a hardware setting that indicates which card is first, second, and so on, install the cards in the order specified by the hardware settings.
- If you are installing voice cards of different models in the same server, install cards of the same model adjacent to one another.
- Choose a physically compatible slot in an appropriate bus segment. Refer to the manufacturer documentation for detailed PCI bus topology information.

**Caution**

Placing a 33-MHz Intel Dialogic voice card in a physical interface slot in the same logical segment as a 66-MHz PCI or 100-to-133-MHz PCI-X interface card will slow both slots in the logical segment to 33 MHz, degrading performance of the whole platform.

Step 7 If you are installing multiple voice cards that have H.100 bus connectors, cable the cards together. On each card, connect the cable so the red stripe on the cable corresponds with pin 1 on the card connector. Confirm that the connectors are firmly seated.

**Caution**

If you do not cable cards together as required, the voice card software will not start, and Cisco Unity will not answer calls.

If the cable has more connectors than the server has voice cards, use the first and last connectors, and leave unused connectors in the middle of the cable. If the end of a cable is allowed to dangle loose, it can act as a radio antenna and pick up noise from the bus.

If you are cabling three or more cards together, connect the first connector on the cable to the first card, the second connector to the second card, and so on.

Attaching Peripheral Devices and Making Connections from the Phone System

We recommend that you connect the Cisco Unity server to a dedicated uninterruptible power supply.

A Cisco Unity server purchased from Cisco is configured for a specific hardware setup. Do not add or change any hardware on the server, except to add voice cards, memory, a tape drive, an external modem, or a rail kit.

To Attach Peripheral Devices and to Make Connections from a Circuit-Switched Phone System

Step 1 Place the server in a dry, cool area that is free of dust. Note the following considerations, as applicable:

- If the Cisco Unity server will be connected to the network, place it near a network connection.

- If the Cisco Unity system is using voice cards to integrate with a circuit-switched phone system, place the server near the phone system.
- If the Cisco Unity system is using PIMG units to integrate with a circuit-switched phone system, place the PIMG units near the phone system and near a network connection.



Caution Do not attach the network cable to the server until you have installed the Microsoft service packs and updates recommended for use with Cisco Unity. The Cisco Unity installation guide alerts you when to install the service packs and updates, and when to connect to the network later in the installation process.

- Step 2** Attach any supported peripheral devices to the server. Follow the manufacturer installation and test instructions.
- Step 3** *If Cisco Unity is integrated with a circuit-switched phone system:* Make the necessary connections from the phone system. See the applicable integration guide.
- Cisco Unity integration guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.
- For pinout information, see the “[Voice Cards and PIMG Units](#)” appendix.
- Step 4** *If Cisco Unity is integrated with a circuit-switched phone system, you are installing the Cisco Unity system outside the United States, and the server contains voice cards that came with a ferrite clamp:* Attach the clamp around the analog phone lines as close to the server as possible.
-



CHAPTER 4

Installing the Operating System

In this chapter, you do the following tasks in the order listed:

1. Review considerations for installing Windows. See the [“Considerations for Installing Windows” section on page 4-2](#).
2. *If you are installing Windows by using a retail Windows disc:* Configure the RAID arrays. See the [“Configuring the RAID Arrays \(Selected Installations\)” section on page 4-3](#).
3. Install Windows Server 2003 or Windows 2000 Server by using the applicable procedure based on the considerations you reviewed in Task 1.:
 - [Installing Windows Server 2003 by Using the Cisco Unity Platform Configuration Discs, page 4-4](#)
 - [Installing Windows 2000 Server by Using the Cisco Unity Platform Configuration Discs, page 4-6](#)
 - [Installing Windows Server 2003 by Using a Retail Windows Server 2003 Disc, page 4-8](#)
 - [Installing Windows 2000 Server by Using a Retail Windows Server 2000 Disc, page 4-9](#)
4. *If you installed Windows by using a retail Windows disc:* Create the partitions according to the storage configuration requirements for the platform. See the [“Creating the Partitions” section on page 4-11](#).

If you installed Windows by using the Platform Configuration discs, partitions of the correct sizes were created automatically.
5. *If the Cisco Unity server will have more than 96 ports:* Add the 3GB and userva switches to the boot.ini file. See the [“Adding 3GB and userva Switches to the Boot.ini File” section on page 4-12](#).

When you are finished with this chapter, return to [Chapter 1, “Overview of Mandatory Tasks for Installing Cisco Unity,”](#) to continue installing the Cisco Unity system correctly.



Note

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Considerations for Installing Windows

In general, we recommend that you install Windows Server 2003 on the Cisco Unity server. Microsoft will produce service packs and security updates for Windows Server 2003 for several years longer than it does for Windows 2000 Server.

Note the considerations in the following sections:

- [Windows Server 2003 Considerations, page 4-2](#)
- [Windows 2000 Server Considerations, page 4-2](#)
- [Additional Considerations for Both Windows Versions, page 4-2](#)

Windows Server 2003 Considerations

- If Windows Server 2003 is installed on the Cisco Unity server, voice cards and Dialogic software will not function correctly. Consequently, circuit-switched phone system integrations that use voice cards are not supported for use with a Cisco Unity server on which Windows Server 2003 is installed. (IP integrations—Cisco Unified CM and SIP—and PIMG integrations are supported for use with a Cisco Unity server on which Windows Server 2003 is installed.)
- The Cisco Unity Platform Configuration discs for all servers install the Windows Server 2003 Multilingual User Interface (MUI) as well as Windows in English. The MUI allows you to change the language of the Windows user interface to the other operating-system languages supported for use with Cisco Unity: French, German, and Japanese.

Windows 2000 Server Considerations

The Cisco Unity Platform Configuration discs install Windows 2000 Server in English and do not install the Multilingual User Interface (MUI). If you want to display the Windows 2000 Server user interface in French, German, or Japanese, you must install Windows by using one of the following discs:

- A localized installation disc. You must purchase a retail Windows 2000 Server disc localized in the desired language.
- A Windows 2000 Server disc that includes the MUI, which is available only through Microsoft volume-licensing programs. The MUI allows you to change the language of the Windows user interface to the other operating-system languages supported for use with Cisco Unity: French, German, and Japanese.

Additional Considerations for Both Windows Versions

- If you install Windows by using the Cisco Unity Platform Configuration discs or an English-language retail disc, you must install the English-language version of all third-party software on the Cisco Unity server.
- The Cisco Unity Server Updates wizard, which automatically installs the latest Microsoft updates recommended for use with Cisco Unity, installs only English-language updates. You can use the Server Updates wizard to install updates only in the following cases:
 - You installed Windows by using the Platform Configuration discs.
 - You installed Windows by using an English-language retail disc, with or without the MUI.

If you install a non-English version of Windows, you cannot use the Server Updates wizard to install updates. We recommend that you download the updates from the Microsoft website and manually install them, or download and install them by using Windows Automatic Update. (For more information on Windows Automatic Update, refer to the “Support Policy for Windows Automatic Update” section in *Supported Hardware and Software, and Support Policies for Cisco Unity Release 5.x*. For a list of the updates currently recommended for use with Cisco Unity, refer to *Software Installed by the Cisco Unity Server Updates Wizard*. Both documents are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.)

Configuring the RAID Arrays (Selected Installations)

If you are installing Windows using the Cisco Unity Platform Configuration discs, or if the system is not using RAID, skip this section.

Do this section only if the system is using hardware-based RAID. (Software-based RAID is not supported.)

To configure the arrays, you group the physical disks into logical disks and assign a RAID type to each logical disk. The server manufacturer provides a disc that contains utilities for several setup tasks, including configuring RAID arrays. Use the disc to configure the arrays when the Cisco Unity server was not purchased from Cisco.

The following discs are provided by server manufacturers:

Hewlett-Packard	Hewlett-Packard SmartStart
IBM	IBM ServerGuide (Windows Server 2003 only)

The following procedure contains only general steps. For detailed instructions on using a specific array-configuration utility, refer to the manufacturer documentation.

To Configure the RAID Arrays by Using the Manufacturer-Provided Utility

-
- Step 1** Start the Cisco Unity server, and insert the manufacturer disc in the DVD drive.
 - Step 2** On the main menu, select the array-configuration utility.
 - Step 3** For each logical disk needed, group physical disks of the same make and model, and assign a RAID type.
For information on the recommended RAID configuration for the server, refer to the *Cisco Unity Supported Platforms List* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.
 - Step 4** Follow the manufacturer instructions to complete the configuration.
-

Installing Windows Server 2003 by Using the Cisco Unity Platform Configuration Discs

A Cisco Unity server purchased from Cisco ships with Platform Configuration discs that contain a utility to install Windows Server 2003 by restoring an image that is customized for the platform. The image includes the Windows Server 2003 components, subcomponents, and service packs that were required by the version of Cisco Unity that was shipping at the time that the Platform Configuration discs were created.

Installing Windows Server 2003 by using the Cisco Unity Platform Configuration discs reduces the Cisco Unity system installation time and ensures that the required operating system and components, drivers, and service packs are installed and configured correctly. In addition, the partitions are automatically set up.



Caution

Do not attach the network cable to the server until you have installed the Microsoft service packs and updates recommended for use with Cisco Unity. The Cisco Unity installation guide alerts you when to install the service packs and updates, and when to connect to the network later in the installation process.

To Install Windows Server 2003 by Using the Cisco Platform Configuration Disc (Selected Servers Only)

Step 1 Remove any devices that are connected to a USB port on the server.



Caution

If you leave USB devices plugged into the server during Windows configuration, the devices may be interpreted as storage devices. As a result, Windows will not create hard-disk partitions that are required by Cisco Unity Setup, and Setup will fail.

Step 2 Start the server, and insert the Cisco Unity Platform Configuration disc in the DVD drive.

Step 3 Restart the server.

Step 4 If you are using a server manufactured by Hewlett-Packard, skip to [Step 5](#).

If you are using a server manufactured by IBM and the following message appears:

“The ServeRAID firmware and BIOS installed on your system must be upgraded or downgraded to be compatible with the RAID drivers on the Cisco Platform Configuration disc. For information on upgrading or downgrading, refer to the Cisco Technical Note [Upgrading or Downgrading ServeRAID Firmware and BIOS on IBM Servers on Cisco.com](#).”

do the procedures in the tech note *RAID-Controller Firmware and RAID BIOS on IBM Servers Upgrade or Downgrade Procedure* at

http://www.cisco.com/en/US/products/ps6509/tsd_products_support_install_and_upgrade_technotes_list.html (the document title changed). Then return to [Step 2](#) of this procedure.

If you are using an MCS-7815I-3.0-ECS1 or MCS-7815-I1-ECS1 server and the server will not boot from the Cisco Unity Platform Configuration disc, do the procedures in the tech note *MCS-7815I-3.0-xxx1 and MCS-7815-I1-xxx1 (Shipped Before March 2005) DVD-ROM Drive Does Not Consistently Boot* at

http://www.cisco.com/en/US/products/ps6509/tsd_products_support_install_and_upgrade_technotes_list.html. Then return to [Step 2](#) of this procedure.

Step 5 If you are using a server manufactured by IBM, skip to [Step 6](#).

If you are using a server manufactured by Hewlett-Packard, choose a language for the operating system and the locale.

The remaining Windows Server 2003 installation screens will be in English, but when the Windows installation is complete, the Windows user interface will display in the language you selected.

Step 6 Follow the on-screen prompts until you are prompted to choose a licensing mode.

Step 7 Click **Per Server**, and click **Next**.

Step 8 Enter a name for the server (netBIOS name). Use only alphabetical characters A to Z and a to z, numerical characters 0 to 9, and hyphens (-). We recommend that you assign a name with 15 or fewer characters.

**Caution**

Using other characters in the server name is not supported by DNS.

If there is more than one Cisco Unity server in an Active Directory forest, give each Cisco Unity server a name that is unique in the first 14 characters, or Cisco Unity will have problems communicating with the Active Directory accounts that it creates. For example, the following names would cause communication problems: CiscoUnitySrvr1 and CiscoUnitySrvr2.

Step 9 Click **Next**.

Step 10 Enter and confirm a password for the Administrator account.

**Caution**

If you are using a server manufactured by Hewlett-Packard and you chose a language other than English in [Step 5](#), note that until Windows installation has finished, the keyboard layout is the English-language QWERTY keyboard layout, not the standard keyboard layout for the language you chose.

Step 11 Click **Next**.

Step 12 Follow the on-screen prompts until the Workgroup or Computer Domain page appears.

Step 13 Click **No, This Computer Is Not on a Network, or Is on a Network without a Domain**.

Step 14 Optionally, specify a different name for the workgroup.

Step 15 Click **Next**.

Step 16 If you are using a server manufactured by Hewlett-Packard, skip to [Step 17](#).

If you are using a server manufactured by IBM, choose a language for the operating system and the locale.

Step 17 Restart the server.

Step 18 Wait until the Platform Configuration disc has finished running configuration scripts and automatically restarting the server. (There may be multiple automatic restarts.)

Installing Windows 2000 Server by Using the Cisco Unity Platform Configuration Discs

A Cisco Unity server purchased from Cisco ships with Platform Configuration discs that contain a utility to install Windows 2000 Server by restoring an image that is customized for the platform. The image includes the Windows 2000 Server components, subcomponents, and service packs that were required by the version of Cisco Unity that was shipping at the time that the Platform Configuration discs were created.

Installing Windows 2000 Server by using the Cisco Unity Platform Configuration discs reduces the Cisco Unity system installation time and ensures that the required operating system and components, drivers, and service packs are installed and configured correctly. In addition, the logical drives are automatically set up.



Caution

Do not attach the network cable to the server until you have installed the Microsoft service packs and updates recommended for use with Cisco Unity. The Cisco Unity installation guide alerts you when to install the service packs and updates, and when to connect to the network later in the installation process.

Do one of the following two procedures, depending on the platform: Hewlett-Packard or IBM.

Hewlett-Packard: To Install Windows 2000 Server by Using the Cisco Unity Platform Configuration Discs

- Step 1** Start the Cisco Unity server, and insert Cisco Unity Platform and RAID Configuration Disc (HP) CD 1 in the DVD drive.
- Step 2** When the main menu appears, press <F2>.
- Step 3** Follow the on-screen prompts until you are prompted to select a licensing mode.
- Step 4** Click **Per Seat**, and click **Next**.
- Step 5** Enter a name for the server (netBIOS name). Use only alphabetical characters A to Z and a to z, numerical characters 0 to 9, and hyphens (-).



Caution

Using other characters in the server name is not supported by DNS.

If there is more than one Cisco Unity server in an Active Directory forest, give each Cisco Unity server a name that is unique in the first 14 characters, or Cisco Unity will have problems communicating with the Active Directory accounts that it creates. For example, the following names would cause communication problems: CiscoUnitySrvr1 and CiscoUnitySrvr2.

- Step 6** Specify and confirm a password, then click **Next**.
- Step 7** Follow the on-screen prompts until the Network Settings dialog box appears.
- Step 8** Click **Typical Settings**, and click **Next**.
- Step 9** In the Workgroup or Computer Domain dialog box, click **No, This Computer Is Not on a Network, or Is on a Network Without a Domain**.

If the Workgroup or Computer Domain dialog box is empty, enter a workgroup name. The name you enter now is not important. You will join a domain or make the Cisco Unity server a domain controller in a later procedure, so the Cisco Unity server will no longer be in a workgroup.

- Step 10** Click **Next**.

- Step 11** Follow the on-screen prompts to complete the installation.
 - Step 12** When the Windows 2000 Configure Your Server dialog box appears, click **I Will Configure This Server Later**, and click **Next**.
 - Step 13** Uncheck the **Show This Screen at Startup** check box, and close the window.
-

IBM: To Install Windows 2000 Server by Using the Cisco Unity Platform Configuration Discs

- Step 1** Start the Cisco Unity server, and insert Cisco Unity Platform Configuration Disc (IBM) CD 1 in the DVD drive.
- Step 2** When the main menu appears, press **Enter** to start the installation program.
- Step 3** Follow the on-screen prompts until you are prompted to select a licensing mode.
- Step 4** Click **Per Seat**, and click **Next**.
- Step 5** Enter a name for the server (netBIOS name). Use only alphabetical characters A to Z and a to z, numerical characters 0 to 9, and hyphens (-).



Caution Using other characters in the server name is not supported by DNS.

If there is more than one Cisco Unity server in an Active Directory forest, give each Cisco Unity server a name that is unique in the first 14 characters, or Cisco Unity will have problems communicating with the Active Directory accounts that it creates. For example, the following names would cause communication problems: CiscoUnitySrvr1 and CiscoUnitySrvr2.

- Step 6** Specify and confirm a password, then click **Next**.
- Step 7** Follow the on-screen prompts until the Network Settings dialog box appears.
- Step 8** Click **Typical Settings**, and click **Next**.
- Step 9** In the Workgroup or Computer Domain dialog box, click **No, This Computer Is Not on a Network, or Is on a Network Without a Domain**.

If the Workgroup or Computer Domain box is empty, enter a workgroup name. The name you enter now is not important. You will join a domain or make the Cisco Unity server a domain controller in a later procedure, so the Cisco Unity server will no longer be in a workgroup.

- Step 10** Click **Next**.
 - Step 11** Follow the on-screen prompts to complete the installation.
 - Step 12** When the Windows 2000 Configure Your Server dialog box appears, click **I Will Configure This Server Later**, and click **Next**.
 - Step 13** Uncheck the **Show This Screen at Startup** check box, and close the window.
-

Installing Windows Server 2003 by Using a Retail Windows Server 2003 Disc

The server manufacturer provides a disc that contains utilities for several setup tasks, including guiding the installation of Windows 2003 Server from a retail disc. Always use the manufacturer's guided system-setup utility to install Windows Server 2003. This ensures that the operating system and the drivers are installed and configured correctly.



Caution

When installing Windows Server 2003, do not install Universal Description, Discovery, and Integration (UDDI) Services, or the Cisco Unity System Preparation Assistant will fail later in the installation process.

The following discs are provided by server manufacturers:

Hewlett-Packard	Hewlett-Packard SmartStart
IBM	IBM ServerGuide



Caution

Do not attach the network cable to the server until you have installed the Microsoft service packs and updates recommended for use with Cisco Unity. The Cisco Unity installation guide alerts you when to install the service packs and updates, and when to connect to the network later in the installation process.

To Install Windows Server 2003 by Using the Manufacturer's Guided System-Setup Utility and a Retail Windows 2003 Disc

-
- Step 1** Start the Cisco Unity server, and insert the manufacturer disc in the DVD drive.
- Step 2** Follow the on-screen prompts to install Windows Server 2003 from a retail disc.
- You may be prompted to configure the RAID arrays. Note the following considerations:
- If the arrays have already been configured, do not change the configuration.
 - If the arrays have not been configured, follow the prompts to configure them. Refer to the manufacturer documentation.
- Step 3** When applicable, make the following choices:
- Specify a partition size of **12 GB** for the operating system.
 - If you are installing Windows Server 2003 on the same partition where an operating system is already installed, select and delete that partition.

- Format the operating system partition by using the **NTFS** file system.
- For regional settings, select a locale in the Your Locale (Location) list. The locale you select must match one of the system-prompts languages that you will install for Cisco Unity. Note that Cisco Unity Setup always installs the English (United States) system prompts.

For a list of supported system-prompts languages, refer to the “Available Languages for Cisco Unity Components” section in the applicable version of *Release Notes for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

**Caution**

If the locale you specify when you install Windows Server 2003 does not match any of the installed Cisco Unity system-prompts languages, Cisco Unity will log errors in the event log and may stop taking calls. The locale you select here must match the Cisco Unity system-prompt language exactly. For example, if you choose English (United Kingdom) for locale, you must also choose English (United Kingdom) as one of the Cisco Unity system-prompts languages. Installing the system prompts for English (Australia) will not work.

- Specify **Per Seat** for the licensing mode.
- When you enter a name (netBIOS name) for the Cisco Unity server:
 - If there is more than one Cisco Unity server in an Active Directory forest, give each Cisco Unity server a name that is unique in the first 14 characters, or Cisco Unity will have problems communicating with the Active Directory accounts that it creates. For example, the following names would cause communication problems: CiscoUnitySrvr1 and CiscoUnitySrvr2.
 - Use only alphabetical characters A to Z and a to z, numerical characters 0 to 9, and hyphens (-).

**Caution**

Using other characters in the server name is not supported by DNS.

- Do not join a domain. Instead, specify a workgroup. The Cisco Unity installation guide alerts you when to connect to the network and when to join a domain later in the installation process.

Installing Windows 2000 Server by Using a Retail Windows Server 2000 Disc

The server manufacturer provides a disc that contains utilities for several setup tasks, including guiding the installation of Windows 2000 Server from a retail disc. Use the manufacturer disc when the Cisco Unity server was not purchased from Cisco.

The following discs are provided by server manufacturers:

Hewlett-Packard	Hewlett-Packard SmartStart
IBM	IBM ServerGuide (selected servers only)

Installing Windows 2000 Server by using the manufacturer’s guided system-setup utility ensures that the operating system and the drivers are installed and configured correctly.

**Caution**

Do not attach the network cable to the server until you have installed the Microsoft service packs and updates recommended for use with Cisco Unity. The Cisco Unity installation guide alerts you when to install the service packs and updates, and when to connect to the network later in the installation process.

To Install Windows 2000 Server by Using the Manufacturer's Guided System-Setup Utility and a Retail Windows 2000 Disc

Step 1 Start the Cisco Unity server, and insert the manufacturer disc in the DVD drive.

Step 2 Follow the on-screen prompts to install Windows 2000 Server from a retail disc.

You may be prompted to configure the RAID arrays. Note the following considerations:

- If the arrays have already been configured, do not change the configuration.
- If the arrays have not been configured, follow the prompts to configure them. Refer to the manufacturer documentation.

Step 3 When applicable, make the following choices:

- Specify a partition size of **12 GB** for the operating system.
- If you are installing Windows 2000 Server on the same partition where an operating system is already installed, select and delete that partition.
- Format the operating system partition by using the **NTFS** file system.
- For regional settings, select a locale in the Your Locale (Location) list. The locale you select must match one of the system-prompts languages that you will install for Cisco Unity. Note that Cisco Unity Setup always installs the English (United States) system prompts.

For a list of supported system-prompts languages, refer to the “Available Languages for Cisco Unity Components” section in the applicable version of *Release Notes for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

**Caution**

If the locale you specify when you install Windows 2000 Server does not match any of the installed Cisco Unity system-prompts languages, Cisco Unity will log errors in the event log and may stop taking calls. The locale you select here must match the Cisco Unity system-prompt language exactly. For example, if you choose English (United Kingdom) for locale, you must also choose English (United Kingdom) as one of the Cisco Unity system-prompts languages. Installing the system prompts for English (Australia) will not work.

- Specify **Per Seat** for the licensing mode.
- When you enter a name for the Cisco Unity server (netBIOS name), use only alphabetical characters A to Z and a to z, numerical characters 0 to 9, and hyphens (-).

**Caution**

Using other characters in the server name is not supported by DNS.

If there is more than one Cisco Unity server in an Active Directory forest, give each Cisco Unity server a name that is unique in the first 14 characters, or Cisco Unity will have problems communicating with the Active Directory accounts that it creates. For example, the following names would cause communication problems: CiscoUnitySrvr1 and CiscoUnitySrvr2.

- Do not join a domain. Instead, specify a workgroup. The Cisco Unity installation guide alerts you when to connect to the network and when to join a domain later in the installation process.
- If you are prompted to specify Windows 2000 Server components to install, select the following required components:
 - Internet Information Services
 - Message Queuing Services



Note If you do not install all the required Windows 2000 Server components, subcomponents, and service packs while installing the operating system, the Cisco Unity installation guide alerts you when and how to install them later.

- Step 4** When the Windows 2000 Configure Your Server dialog box appears, click **I Will Configure This Server Later**.
- Step 5** Uncheck the **Show This Screen at Startup** check box, and close the window.

Creating the Partitions



Note If the Cisco Unity server was purchased from Cisco, skip this section. When you installed Windows using the Cisco Unity Platform Configuration discs shipped with the server, the partitions were created automatically.

Do the following procedure to create the partitions that you identified in the [“Determining the Locations for Files on the Cisco Unity Server”](#) section on page 2-4.

To Create the Partitions

- Step 1** Log on to Windows as a member of the Administrators group.
- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Computer Management**.
- Step 3** In the console tree under Storage, click **Disk Management**.
- Step 4** Right-click the first available unallocated region of the first available logical disk, and click **New Partition** (if Windows Server 2003 is installed) or **Create Partition** (if Windows 2000 Server is installed).
- Typically, you will need to create one more partition than the number of logical disks available. After you install the operating system, the first 12 GB of the first logical disk is used for the system partition, and is given the drive letter C. You create the first extended partition by using the remaining space on the first logical disk. When you create subsequent partitions, you use the entire logical disk.
- Step 5** On the New Partition Wizard (Windows Server 2003) or Create Partition Wizard (Windows 2000 Server) welcome screen, click **Next**.
- Step 6** Click **Extended Partition**, and click **Next**. (Do not click Primary Partition.)
- Step 7** Specify to use the remaining disk space, and click **Next**.
- Step 8** Verify the settings, and click **Finish**.

- Step 9** In the Disk Management utility, right-click the new partition, and click **New Logical Drive** (Windows Server 2003) or **Create Logical Drive** (Windows 2000 Server).
 - Step 10** On the Create Partition Wizard welcome screen, click **Next**.
 - Step 11** Click **Logical Drive**, and click **Next**.
 - Step 12** Specify to use the maximum disk space, and click **Next**.
 - Step 13** Assign a drive letter, and click **Next**.
 - Step 14** Specify the NTFS file system format, and click **Next**.
 - Step 15** Verify the settings, and click **Finish**.
 - Step 16** Repeat [Step 4](#) through [Step 15](#) for each partition that you have to create.
-

Adding 3GB and userva Switches to the Boot.ini File

If the Cisco Unity server will be configured for more than 96 voice messaging ports, do the following procedure.

To Add 3GB and userva Switches to the Boot.ini File

- Step 1** Open the `c:\boot.ini` file in a text editor.
 - Step 2** Add `/3GB /userva=2800` to the line that includes `WINDOWS="Microsoft Windows 2003 Server"`. For example:


```
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Standard" /fastdetect /NoExecute=OptOut /3GB /userva=2800
```
 - Step 3** Restart the server.
-



CHAPTER 5

Customizing the Cisco Unity Platform

In this chapter, you do the following tasks in the order listed:

1. *If the Cisco Unity server contains a dual NIC:* Configure the dual NIC or verify the configuration. See the [“Configuring a Dual NIC in the Cisco Unity Server”](#) section on page 5-2.
2. Complete registration information on Cisco.com to obtain the applicable license files. See the [“Obtaining Cisco Unity License Files”](#) section on page 5-4.
3. Use the Cisco Unity System Preparation Assistant to install required Windows components, the browser and database, and required service packs. See the [“Running the Cisco Unity System Preparation Assistant”](#) section on page 5-6.
4. *If the system is using MSDE 2000:* Install Enterprise Manager, and set the MSDE system administrator password. See the [“Installing Administration Software for MSDE 2000 and Setting the MSDE System Administrator Password”](#) section on page 5-9.
5. Change folder settings in Windows Explorer so that all files and folders are visible during Cisco Unity troubleshooting, if applicable. See the [“Changing Folder Settings in Windows Explorer”](#) section on page 5-10.
6. Run the Cisco Unity Server Updates wizard to install Microsoft security updates and, optionally, Cisco Security Agent for Cisco Unity. See the [“Installing Microsoft Updates and Cisco Security Agent for Cisco Unity”](#) section on page 5-10.



Caution

Do not install the latest service packs that are recommended for use with Cisco Unity yet. Any service packs qualified for use with the current version of Cisco Unity after the current version was released have not been tested with Cisco Unity Setup and may cause Setup to fail.

7. *If the Cisco Unity server contains voice cards:* Disable the Found New Hardware wizard, if applicable. See the [“Disabling the Found New Hardware Wizard for the Voice Cards”](#) section on page 5-11.
8. *Optional:* Install antivirus software. See the [“Installing Antivirus Software \(Optional\)”](#) section on page 5-12.
9. Connect the Cisco Unity server to the network. See the [“Connecting the Cisco Unity Server to the Network”](#) section on page 5-12.

10. Configure TCP/IP properties. See the [“Configuring TCP/IP Properties”](#) section on page 5-12.
11. Confirm that the server has a valid IP address and is connected to the network. See the [“Verifying the IP Address and the Network Connection”](#) section on page 5-13.
12. *If antivirus software or Cisco Security Agent for Cisco Unity is installed on the Cisco Unity server:* Disable virus-scanning and Cisco Security Agent for Cisco Unity services. See the [“Disabling Antivirus and Cisco Security Agent Services”](#) section on page 5-14.
13. Install Microsoft Active Directory, or add the Cisco Unity server to an existing domain. See the [“Installing Active Directory or Adding the Cisco Unity Server to an Existing Domain”](#) section on page 5-15.

When you are finished with this chapter, return to [Chapter 1, “Overview of Mandatory Tasks for Installing Cisco Unity”](#) to continue installing the Cisco Unity system.

**Note**

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Configuring a Dual NIC in the Cisco Unity Server

**Note**

If the Cisco Unity server does not contain a dual NIC, skip this section.

We recommend that a dual NIC be configured in adapter fault tolerant mode (AFT) or network fault tolerant (NFT) mode. One NIC is designated as the primary and the other NIC as the secondary for active-passive fault tolerance. In this configuration, the primary (active) NIC handles 100 percent of the traffic. Only in the event that the primary NIC becomes unavailable does the secondary NIC then become active and handle 100 percent of the traffic.

Alternatively, if you do not want to configure AFT or NFT, or do not have a second LAN port available, the following configurations are supported, though not recommended:

- Disable TCP/IP for the second NIC, which allows you to re-enable the second NIC remotely if the first NIC fails. (Use the Network and Dial-up Connections Control Panel to disable TCP/IP for the second NIC.)
- Disable the second NIC in the BIOS. (On some Cisco Unity servers, the second NIC is disabled in the BIOS by default.)

**Caution**

Not plugging a network cable into the second NIC is not sufficient. You must either disable TCP/IP for the second NIC or disable the second NIC in the BIOS, or Cisco Unity may not work properly.

If you installed Windows by using the Cisco Unity Platform Configuration discs, skip to the [“Configuring a Dual NIC”](#) section on page 5-4. (The NIC-configuration utility was installed automatically.)

If you installed Windows by using a retail Windows disc, you need to install the NIC-configuration utility before you can configure the dual NIC. Do the applicable procedures in the following two sections, [“Installing the NIC-Configuration Utility”](#) and [“Configuring a Dual NIC.”](#)

Installing the NIC-Configuration Utility

**Note**

If you installed Windows by using the Cisco Unity Platform Configuration discs, skip this section.

Do the applicable procedure in this section, depending on whether the Cisco Unity server was manufactured by Hewlett-Packard or IBM and, for IBM, depending on whether you have an Intel or a Broadcom installation disc (the disc corresponds with the brand of NIC installed in the server):

- [To Install the Hewlett-Packard NIC-Configuration Utility, page 5-3](#)
- [To Install the IBM NIC-Configuration Utility by Using a Broadcom Disc, page 5-3](#)
- [To Install the IBM NIC-Configuration Utility by Using an Intel Disc, page 5-4](#)

(Cisco-branded servers that have a model number ending in “H” were manufactured by Hewlett-Packard. Cisco-branded servers that have a model number ending in “I” were manufactured by IBM.)

**Note**

The following procedures are intended for the software shipped with the Cisco Unity servers that were shipping at the time this document was published. Procedures for older or newer servers may differ.

To Install the Hewlett-Packard NIC-Configuration Utility

- Step 1** Insert the Hewlett-Packard SmartStart disc in the DVD drive.
- Step 2** Browse to the directory **Compaq\Csp\Nt**, and double-click **Setup.exe**.
- Step 3** In the right pane of the HP Remote Deployment utility, select and delete all items except HP ProLiant Network Configuration Utility <version> for Windows <2003/2000>.
- Step 4** Click **Install**.
- Step 5** Follow the on-screen prompts to complete the installation.

To Install the IBM NIC-Configuration Utility by Using a Broadcom Disc

- Step 1** Insert the Broadcom NetXtreme Gigabit Ethernet Software disc in the DVD drive.
If the installation program does not appear automatically, browse to the root of the CD, and double-click **Launch.exe**.
- Step 2** In the installation program, click **Management Programs**.
- Step 3** Follow the on-screen prompts until you are prompted to select the applications to install.
- Step 4** Check the **Control Suite** and **BASP** check boxes.
- Step 5** Follow the on-screen prompts to complete the installation.

To Install the IBM NIC-Configuration Utility by Using an Intel Disc

-
- Step 1** Insert the Intel Ethernet Software disc in the DVD drive.
- If the installation program does not appear automatically, browse to the root of the CD, and double-click **Autorun.exe**.
- Step 2** Follow the on-screen prompts to complete the installation.
-

Configuring a Dual NIC

To Configure a Dual NIC in the Cisco Unity Server

-
- Step 1** Start the NIC-configuration utility:
- On the Windows Start menu, click **Settings > Control Panel**.
 - Choose the applicable option, depending on the server model and NIC brand:

Hewlett-Packard or Cisco MCS server with model number ending in "H"	Click HP Network .
IBM or Cisco MCS server with model number ending in "I"	<ul style="list-style-type: none"> For a Broadcom dual NIC, click Broadcom Control Suite 2. For an Intel dual NIC, click Intel(R) PROSet Wired.

- Step 2** Configure the dual NIC—or verify the configuration—so that the following conditions are met:
- Both NICs are connected to the same network segment (in other words, both are connected to the same Layer 3 subnet and the same Layer 2 Ethernet broadcast domain).
 - Both share the same IP address.
 - Both are set up for AFT or for NFT. Refer to the NIC-configuration utility Help.
- Step 3** Write down the MAC address that now applies to both NICs. You will need it when you obtain license files in the [“Obtaining Cisco Unity License Files” section on page 5-4](#).
- Step 4** Restart the Cisco Unity server for any changes to take effect.
-

Obtaining Cisco Unity License Files

License files, which enable the features purchased by the customer, are required for installing Cisco Unity software, for some upgrades, and for adding or changing licensed features. You obtain the license files by completing registration information on Cisco.com.

Shortly after registration, Cisco e-mails the license files. The e-mail from Cisco contains instructions on how to save and store the files. The Cisco Unity installation guide later provides specific instructions on the use of the license files. (For more information on licensing, refer to the white paper *Licensing for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html.)

The following information is required during registration:

- The MAC address (physical address) for the network interface card (NIC) in the Cisco Unity server.
- The product authorization key (PAK), which appears on the sticker located on the front of the sleeve for Cisco Unity DVD 1.

If the server contains a dual NIC and you configured it for fault tolerance by using the procedure in the “Configuring a Dual NIC in the Cisco Unity Server” section on page 5-2, you already have the MAC address. Skip to the “To Register and Obtain the License Files” procedure on page 5-5.

If the server contains one NIC or if the server contains a dual NIC that you did not configure for fault tolerance, do the following two procedures in the order listed.

To Get the MAC Address of the Cisco Unity Server When the Server Contains One NIC or an Unteamed Dual NIC

- Step 1** On the server on which Cisco Unity will be installed, on the Windows Start menu, click **Programs > Accessories > Command Prompt**.
- Step 2** In the Command Prompt window, enter **ipconfig /all**, and press **Enter**.
- Step 3** Write down the value of Physical Address, excluding the hyphens, or save it to a file that you can access during online registration. (For example, if the physical address is 00-A1-B2-C3-D4-E5, record 00A1B2C3D4E5.)
- If the server contains a dual NIC, two values will appear. Write down the value for the NIC that you will use to connect the Cisco Unity server to the network.
- Step 4** Close the Command Prompt window.
-

To Register and Obtain the License Files

- Step 1** Browse to the registration website at <http://www.cisco.com/go/license> (URL is case sensitive). You must be a registered user on Cisco.com to obtain license files.
- Step 2** Enter the PAK or software serial number, and click **Submit**.
- Step 3** Follow the on-screen prompts.
- Step 4** Shortly after registration, you will receive an e-mail with the Cisco Unity license files.
- If license files are lost, it can take up to one business day to get another copy.
-

If you do not receive the license files within 1 hour or to get another copy of a license file, call the Cisco Technical Assistance Center (TAC) and ask for the Licensing Team:

In the U.S.	800 553-2447
Outside the U.S.	For your local Cisco TAC phone number, see the Cisco Worldwide Contacts page at http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml .

Or open a service request using the TAC Service Request Tool at <http://tools.cisco.com/ServiceRequestTool/create/DefineProblem.do>.

You will need to provide information to verify Cisco Unity ownership—for example, the purchase order number or the PAK (which appears on the sticker located on the front of the sleeve for Cisco Unity DVD 1 or CD 1).

**Note**

Cisco Unity software comes with a default license file that has a minimal number of settings. The license file allows installation of a Cisco Unity demonstration system. For information and instructions on installing a demonstration system, refer to the “Cisco Unity Demonstration System” section of the Cisco Unity release notes.

Running the Cisco Unity System Preparation Assistant

The Cisco Unity System Preparation Assistant is a program that helps customize the platform for Cisco Unity by checking for and installing Windows components, Microsoft service packs and updates, and other software required by Cisco Unity. (For a detailed list, refer to *Components and Software Installed by the Cisco Unity Platform Configuration Discs and the Cisco Unity System Preparation Assistant* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.)

**Caution**

Do not run the Cisco Unity System Preparation Assistant remotely by using Windows Terminal Services or other remote-access applications, or the installation of required software may fail.

To Run the Cisco Unity System Preparation Assistant

- Step 1** Log on to Windows by using an account that is a member of the local Administrators group.
- Step 2** On Cisco Unity Service Packs CD 1, browse to the **Cuspa** directory, and double-click **Cuspa.vbs**.
If you are accessing the Cisco Unity System Preparation Assistant files on another server, use Windows Explorer or the “net” command to map the network drive to a drive letter on the Cisco Unity server before you run Cuspa.vbs.
- Step 3** If prompted, double-click the language of your choice to continue the installation.
- Step 4** On the Welcome screen, click **Next**.

Step 5 On the Cisco Unity Server Characteristics page, set the following fields:

Configuration	Click Unified Messaging or Voice Messaging Only , as applicable.
Failover	Confirm that the This Is a Primary or Secondary Failover Server check box is unchecked.
Number of Ports	Enter the number of voice ports that you are connecting with the Cisco Unity server. The assistant uses the information to determine whether the system requires SQL Server or MSDE. For systems with more than 32 ports, SQL Server is required. Otherwise, MSDE is required.

Step 6 Click **Next**. The assistant lists the components and indicates whether or not they are installed.

Step 7 Follow the prompts to install any missing components until you are prompted to install the data store. If a Microsoft AutoMenu window appears when the assistant is installing an application, close the window and allow the assistant to continue.

Step 8 If MSDE is being installed, skip to [Step 9](#).

If SQL Server is being installed, install it in the location you made note of in the [“Determining the Locations for Files on the Cisco Unity Server”](#) section on page 2-4:

- a. In the Welcome dialog box, click **Next**.
- b. In the Computer Name dialog box, click **Next** to accept the default setting **Local Computer**.
- c. In the Installation Selection dialog box, click **Next** to accept the default setting **Create a New Instance of SQL Server, or Install Client Tools**.
- d. Follow the on-screen prompts until the CD Key dialog box appears.
- e. Enter the key for Cisco Unity Data Store 2000 from the sticker located on the CD sleeve, and click **Next**.
- f. In the Installation Definition dialog box, click **Next** to accept the default setting **Server and Client Tools**.
- g. In the Instance Name dialog box, check the **Default** check box.
- h. Click **Next**.
- i. In the Setup Type dialog box, click **Typical**.
- j. Under Destination Folder, next to Program Files, click **Browse** and specify the location for binaries that you made note of in the [“Determining the Locations for Files on the Cisco Unity Server”](#) section on page 2-4.
- k. Under Destination Folder, next to Data Files, click **Browse** and specify the location for databases that you made note of in the [“Determining the Locations for Files on the Cisco Unity Server”](#) section on page 2-4.
- l. Click **Next**.
- m. At the top of the Services Accounts dialog box, click **Use the Same Account for Each Service**.
- n. Under Service Settings, click **Use the Local System Account**.
- o. Click **Next**.

- p. In the Authentication Mode dialog box, we recommend that you click **Windows Authentication Mode**.
If you click Mixed Mode—which is supported but is less secure—under Add Password for the SA Login, enter and confirm a password for the SQL Server system administrator logon.
- q. Click **Next**.
- r. In the Start Copying Files dialog box, click **Next**.
- s. In the Choose Licensing Mode dialog box, click **Processor License For**, and specify the number of processors in the Cisco Unity server.
- t. Click **Continue**.
- u. If you are prompted about shutdown tasks before continuing with the installation, click **Next**.
- v. Click **Finish**.
- w. Skip to [Step 10](#).

Step 9 If MSDE is being installed, install it now:

- a. Follow the on-screen prompts.
- b. When the installation is complete, click **Yes** to restart the server.

Step 10 When SQL Server or MSDE installation is complete, continue following the on-screen prompts in the assistant to complete the platform customization.

Step 11 If the MSDE service pack is being installed, skip to [Step 12](#).

If the SQL Server service pack is being installed, install it now:

- a. On the Welcome screen, click **Next**.
- b. Follow the on-screen prompts until you are prompted to choose the authentication mode.
- c. Choose Windows authentication, and click **Next**.
- d. If the SA Password Warning dialog box appears, enter and confirm the password, and click **Next**.
- e. Follow the on-screen prompts to continue.
- f. If you are prompted about shutdown tasks before continuing with the installation, click **Next**.
- g. Click **Finish** to begin installing components.
- h. When the Setup message appears, click **OK**.
- i. Click **Finish** to restart the server.
- j. Skip to [Step 13](#).

Step 12 If the MSDE service pack is being installed, install it now:

- a. Follow the on-screen prompts.
- b. When the installation is complete, click **Yes** to restart the server.

Step 13 Follow the on-screen prompts.

Step 14 When the Cisco Unity System Preparation Assistant has completed, click **Finish**.

Installing Administration Software for MSDE 2000 and Setting the MSDE System Administrator Password

**Note**

If the system is not using MSDE 2000, skip this section.

When the Cisco Unity System Preparation Assistant installs MSDE 2000, it does not include administration software. You install Enterprise Manager administration software so that Cisco TAC can access the Cisco Unity MSDE databases during troubleshooting.

For security reasons, we highly recommend that you set a non-blank MSDE 2000 system administrator (sa) password. By default, the sa password is blank. After you install Enterprise Manager, you can use it to reset the sa password.

Do the following two procedures in the order listed.

To Install Enterprise Manager for MSDE 2000

- Step 1** After the server restarts (it was restarted in the preceding procedure), log on to Windows.
- Step 2** If the Cisco Unity Data Store 2000 CD does not run automatically, browse to the root directory, and double-click **Autorun.exe**.
- Step 3** Click **SQL Server 2000 Components**.
- Step 4** Click **Install Database Server**.
- Step 5** In the Welcome dialog box, click **Next**.
- Step 6** In the Computer Name dialog box, click **Next** to accept the default setting **Local Computer**.
- Step 7** In the Installation Selection dialog box, click **Next** to accept the default setting **Create a New Instance of SQL Server, or Install Client Tools**.
- Step 8** Follow the on-screen prompts until the CD Key dialog box appears.
- Step 9** Enter the key for Cisco Unity Data Store 2000 from the sticker located on the CD sleeve.
- Step 10** Click **Next**.
- Step 11** In the Installation Definition dialog box, click **Client Tools Only**.
- Step 12** Click **Next**.
- Step 13** In the Select Components dialog box, in the Components list, check the **Management Tools** check box and uncheck all other check boxes.
- Step 14** Select **Management Tools** (but do not uncheck the check box).
- Step 15** In the Sub-Components list, check the **Enterprise Manager** check box and uncheck all other check boxes, then click **Next**.
- Step 16** In the Start Copying Files dialog box, click **Next**.
- Step 17** Click **Finish**.

To Set the Sa Password for MSDE

- Step 1** On the Windows Start menu, click **Programs > Microsoft SQL Server > Enterprise Manager**.

- Step 2** In the tree, expand **Console Root\Microsoft SQL Servers\SQL Server Group\ (local)(Windows NT)\Security**.
 - Step 3** Click **Logins**.
 - Step 4** In the right pane, right-click **Sa**, and click **Properties**.
 - Step 5** In the SQL Server Login Properties dialog box, click the **General** tab.
 - Step 6** Under SQL Server Authentication, enter the new password.
 - Step 7** Confirm the password, and click **OK**.
 - Step 8** Close Enterprise Manager.
-

Changing Folder Settings in Windows Explorer

You change folder settings so that all files and folders—including system files—are visible in Windows Explorer during Cisco Unity troubleshooting.

If you installed Windows by using the Platform Configuration discs that are shipped with a Cisco Unity server purchased from Cisco, all files and folders are already visible in Windows Explorer.



Note

If you do not do the following procedure now, Cisco TAC may ask you to do it later.

To Change Folder Settings in Windows Explorer

- Step 1** On the Windows desktop, double-click **My Computer**.
 - Step 2** On the Tools menu, click **Folder Options**.
 - Step 3** Click the **View** tab.
 - Step 4** Click **Show Hidden Files and Folders**.
 - Step 5** Uncheck the **Hide File Extensions for Known File Types** check box.
 - Step 6** Uncheck the **Hide Protected Operating System Files** check box, and click **Yes** to confirm.
 - Step 7** Click **Apply**.
 - Step 8** Click **Like Current Folder**, and click **Yes** to confirm.
 - Step 9** Click **OK**.
-

Installing Microsoft Updates and Cisco Security Agent for Cisco Unity

Revised May 1, 2008

You run the Cisco Unity Server Updates wizard that you downloaded in the [“Downloading Software for the Installation” section on page 2-2](#) to install the Microsoft updates that apply to Cisco Unity and, optionally, to install Cisco Security Agent for Cisco Unity.

To Install Microsoft Updates and, Optionally, Cisco Security Agent for Cisco Unity

- Step 1** Insert in the drive the disc that you burned with the latest version of the Cisco Unity Server Updates Wizard.
- Step 2** Run **ServerUpdatesWizard.exe**.
- Step 3** Follow the on-screen prompts to complete the installation of Microsoft updates and, optionally, Cisco Security Agent for Cisco Unity.

**Note**

If you are accessing the server by using Remote Desktop or a VNC client, and you are installing Cisco Security Agent for Cisco Unity, the Remote Desktop or VNC session will be disconnected when Cisco Security Agent for Cisco Unity restarts the network interface. If the session does not reconnect automatically, reconnect manually to finish the Server Updates wizard.

- Step 4** Restart the Cisco Unity server.
-

Disabling the Found New Hardware Wizard for the Voice Cards

**Note**

If the Cisco Unity server does not contain voice cards, skip this section.

In the following cases, the Found New Hardware wizard may appear each time the server is restarted and report that the cards are new hardware, even though the cards are properly installed and configured:

- The operating system was installed by using the Platform Configuration discs.
- The operating system was installed by using the manufacturer's guided system-setup utility before the cards were installed.
- New cards were added to an existing server.

Do the following procedure to prevent the Found New Hardware wizard from reporting the cards as new hardware. The procedure will not prevent the Found New Hardware wizard from finding and reporting other new hardware.

To Disable the Found New Hardware Wizard for the Voice Cards

- Step 1** On the Found New Hardware wizard Welcome page, click **Next**. (After the server is restarted, the Found New Hardware wizard Welcome page is displayed along with the PCI Device Installing dialog.)
- Step 2** On the Install Hardware Device Drivers page, click **Search for a Suitable Driver for My Device (Recommended)**, and click **Next**.
- Step 3** On the Locate Driver Files page, check the **Floppy Disk Drives** and **CD-ROM Drives** check boxes, and click **Next**.
- Step 4** On the Driver Files Search Result page, click **Disable the Device**, and click **Finish**. Do not choose to skip driver installation of this device, or the Found New Hardware wizard will continue to appear each time the server is restarted.

- Step 5** Repeat [Step 2](#) through [Step 4](#) for each instance of the Found New Hardware wizard (for each card, as applicable).

Note that doing this procedure does not prevent a card from being displayed as an unknown PCI device when viewed in the Windows 2000 Device Manager. The warning that the device drivers are not installed also will continue to be displayed. This is expected behavior, and does not indicate a problem with the card or with the server.

Installing Antivirus Software (Optional)

For information on supported antivirus software, refer to *Supported Hardware and Software, and Support Policies for Cisco Unity 5.0* at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Follow the manufacturer instructions to install the antivirus software.

**Caution**

Do not configure antivirus software to block WAV attachments, or voice messages will be stripped of their recordings.

Connecting the Cisco Unity Server to the Network

To Connect the Cisco Unity Server to the Network

Attach the network cable(s) to the Cisco Unity server.

If the server contains a dual NIC, ensure that you connect the cable to the primary NIC, if you configured the dual NIC for AFT or NFT, or to the NIC that is enabled.

Configuring TCP/IP Properties

Revised May 1, 2008

The Cisco Unity server must have an IP address and must also have the IP address of a DNS server. Do the procedure in this section to specify IP addresses for the servers.

When choosing an IP address for a Cisco Unity server, note the following considerations:

- Do not choose an address accessible from the Internet. Doing so can expose the Cisco Unity server to unwanted intrusion from the Internet, even when the server is hardened.
- Do not choose an address that separates the Cisco Unity server from the following servers by a firewall:
 - The Domino server to which Cisco Unity sends voice messages for delivery.
 - The Domino server that Cisco Unity monitors for changes to the directory.

- Any Domino server that homes Cisco Unity subscriber mailboxes.
- The domain controller/global catalog server on which you will create Cisco Unity installation and services accounts in the “[Creating Accounts for the Installation and Granting Permissions](#)” chapter.
- If the Cisco Unity server is separated from any of the following servers by a firewall, open the applicable TCP and UDP ports:
 - DNS servers.
 - Workstations that are used to administer Cisco Unity.
 - Client workstations that will be used to access Cisco Unity via DUC for Cisco and/or the Cisco Personal Communications Assistant (Cisco PCA).
 - Cisco Unified CM servers.
 - SIP end points.
 - SCCP phones.

For details on the TCP/UDP ports that must be opened in a firewall to allow communication between Cisco Unity and other servers, see the “IP Communications Required by Cisco Unity” chapter in the *Security Guide for Cisco Unity 5.x* at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

To Configure TCP/IP Properties

- Step 1** On the Windows Start menu, click **Settings > Control Panel > Network and Dial-Up Connections > Local Area Connection**.
 - Step 2** Click **Properties**.
 - Step 3** In the Components Checked Are Used by This Connection list, check the **Internet Protocol (TCP/IP)** check box.
 - Step 4** Click **Internet Protocol (TCP/IP)** (but do not uncheck the check box), and click **Properties**.
 - Step 5** Enter IP addresses for the Cisco Unity server and for the preferred and alternate DNS servers (for more information, refer to Windows Help).
 - Step 6** Click **OK**.
 - Step 7** Restart the server.
-

Verifying the IP Address and the Network Connection

To Verify the IP Address and the Network Connection

- Step 1** On the Windows Start menu, click **Programs > Accessories > Command Prompt**.
- Step 2** In the Command Prompt window, enter **ipconfig /all**, and press **Enter**.
- Step 3** Verify the IP address of the Cisco Unity server.

- Step 4** Find the IP address of a router or server on the same network segment as the Cisco Unity server.
- If no routers or servers are listed, either you did not specify a default gateway when you assigned an IP address in the “[Configuring TCP/IP Properties](#)” section on page 5-12, or the Cisco Unity server is not connected to the network.
- Step 5** Ping the router or other server whose IP address you found in [Step 4](#). In the Command Prompt window, enter **ping <IP address>**, and press **Enter**.
- If the device sends a reply, the Cisco Unity server has a valid IP address.
- If the device does not reply, there may be a variety of causes. Some of the most common problems include:
- The assigned IP address conflicts with the IP address of another computer on the network.
 - The subnet mask is incorrect.
- Verify the network settings. If needed, troubleshoot any problem as you would a network connectivity problem.
-

Disabling Antivirus and Cisco Security Agent Services



Note

If the system is not using antivirus software or Cisco Security Agent for Cisco Unity, skip this section.

You disable antivirus and Cisco Security Agent services on the server so that they do not slow down the installation of software or cause the installations to fail. The Cisco Unity installation guide alerts you when to re-enable the services after all of the installation procedures that can be affected are complete.

To Disable and Stop Antivirus and Cisco Security Agent Services

- Step 1** Refer to the antivirus software documentation to determine the names of the antivirus services.
- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 3** Disable and stop each antivirus service and the Cisco Security Agent service:
- a. In the right pane, double-click the service.
 - b. On the General tab, in the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.
 - c. Click **Stop** to stop the service immediately.
 - d. Click **OK** to close the Properties dialog box.
- Step 4** When the services have been disabled, close the Services MMC.
-

Installing Active Directory or Adding the Cisco Unity Server to an Existing Domain

The Cisco Unity server must be either a member server in an existing domain or a domain controller in its own domain. Cisco Unity interactions with the message store do not allow the server to be in a workgroup.

If the Cisco Unity server will be the only server in the domain, you must install Active Directory. However, because Active Directory is a very processor- and memory-intensive application, if you are adding the Cisco Unity server to an existing domain, we strongly recommend that you do not also install Active Directory on the Cisco Unity server. Instead, do the procedure in the “Existing Domain” section on page 5-16.

This section contains procedures for installing Active Directory on the Cisco Unity server and for adding the Cisco Unity server as a member server in an existing domain. Do the procedure that is applicable to your installation.

- [Active Directory, page 5-15](#)
- [Existing Domain, page 5-16](#)

Active Directory

Do the following procedure to install Active Directory on the Cisco Unity server and make it a domain controller.

To Install Active Directory on the Cisco Unity Server

-
- Step 1** Log on to the Cisco Unity server by using an account that is a member of the local Administrators group.
- Step 2** On the Windows Start menu, click **Run**, then enter **Dcpromo**, and press **Enter**.
- Step 3** Click **Next**.
- Step 4** Follow the on-screen prompts. Consult the system administrator to determine how to set up the server.
- Step 5** If a DNS message does not appear, skip to [Step 6](#).
- If the message “The wizard cannot contact the DNS server” appears, troubleshoot DNS:
- a. Click **OK** to dismiss the message.
 - b. Click **Cancel** to exit the Active Directory Installation wizard.
 - c. Troubleshoot the current DNS installation.
 - d. Return to [Step 2](#) to start the procedure again.
- Step 6** On the Completing the Active Directory Installation Wizard page, click **Finish**.
- Step 7** Click **Restart Now**.
-

Existing Domain

Do the procedure in this section to add the Cisco Unity server to an existing domain without making it an additional domain controller in that domain.

To Add the Cisco Unity Server to an Existing Domain

- Step 1** Log on to the Cisco Unity server by using an account that is a member of the local Administrators group.
 - Step 2** On the Windows Start menu, click **Settings > Control Panel > System**.
 - Step 3** Click the **Network Identification** tab.
 - Step 4** Click **Properties**.
 - Step 5** In the Identification Changes dialog box, click **Domain**, and enter the name of the domain that you want to join.
 - Step 6** Click **OK**.
 - Step 7** In the Domain Username and Password dialog box, enter the name and password of an account that has permission to add computers to the domain.
 - Step 8** Click **OK** three times.
 - Step 9** Click **Yes** to restart the server.
-



CHAPTER 6

Setting Up Domino and Installing Lotus Notes

In this chapter, you do the following tasks in the order listed:

1. Prepare the Domino server(s) for Cisco Unity. See the “[Preparing the Domino Server\(s\) for Cisco Unity](#)” section on page 6-1.
2. Install and configure IBM Lotus Notes on the Cisco Unity server. See the “[Installing and Configuring Lotus Notes on the Cisco Unity Server](#)” section on page 6-4.

When you are finished with this chapter, return to [Chapter 1](#), “[Overview of Mandatory Tasks for Installing Cisco Unity](#)” to continue installing the Cisco Unity system.



Note

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Preparing the Domino Server(s) for Cisco Unity



Note

Cisco assumes that the Domino environment is already set up and working before the Cisco Unity system is installed.

In the procedure in this section, you:

- Create a Domino group called UnityServers.
- Register a Person with Lotus Notes as the mail system for the Cisco Unity server.
- In the Access Control List (ACL) for Admin4.nsf, grant the UnityServers group Editor permissions.

Admin4.nsf is used by the Administrative Process task running on each Domino server. When a Domino user is imported into Cisco Unity, Cisco Unity submits a signed request to the Adminp task, which adds the request to Admin4.nsf. IBM Lotus Domino Unified Communications (DUC) for Cisco then modifies the user’s mail file with Cisco Unity Unified Messaging functionality. The changes are made to the database on the server that contains the user’s mail file. The UnityServers group requires editor-level permissions in the Admin4.nsf database on each server containing the mail file for a Cisco Unity subscriber.

Domino security policy requires Cisco Unity to digitally sign requests. Requests are documents, and signing documents requires modifying them, so the UnityServers group needs privileges to sign requests submitted to the Administrative Process database. This corresponds to editor-level permissions in an ACL.

- In the Access Control List for Names.nsf, grant the UnityServers group Editor with Delete Documents permissions.

By default, Names.nsf is the main directory database for a Domino domain. Cisco Unity needs sufficient permissions in the ACL of the database to read, edit, create, and delete documents (or “notes”) in the database.

- On the Security tab of the Server document of the Domino address book server, grant the UnityServers group the permission to Create Databases and Templates.

You will specify the Domino server to use as the address book server during Cisco Unity installation in the Cisco Unity Message Store Configuration wizard. The wizard must be able to create mail files for the default accounts, such as the Unity Messaging System account, on the specified Domino server.

- Install DUC for Cisco components on Domino servers.
- Confirm that the network is configured so that Cisco Unity can resolve the unqualified Domino server name to an IP address.

The Cisco Unity server also has Manager-level access to the mail files of its subscribers because when a Domino user is imported into Cisco Unity, DUC for Cisco adds Cisco Unity to the ACL of the mail file for the user. Cisco Unity requires the access to modify the read/unread list. Ensure there are no explicit deny lists or security settings that hinder the ability of Cisco Unity to access a mail file after the Domino user has been imported into Cisco Unity.

To Prepare the Domino Server(s) for Cisco Unity

-
- Step 1** Create a group of type MultiPurpose for the Cisco Unity server, and name it **UnityServers**. Refer to the applicable IBM Lotus documentation.



Note Multipurpose is the recommended type, but Access Control List Only is acceptable.

- Step 2** Register a Person for the Cisco Unity server. Most settings will not affect Cisco Unity functionality, however, you must do the following:

- Create a Lotus Notes mail file for the Person.



Note All Cisco Unity voice messages are submitted to mail.box on the Domino server on which you create the Lotus Notes mail file. Messages are then routed to the Domino servers on which Cisco Unity subscribers are homed. Create the Lotus Notes mail file on a Domino server that is well connected to the network.

- Save the user ID file for the Person in a location other than the Domino directory (the default option). In the Register Person—New Entry dialog box:
 - a. Check the **Advanced** check box, so tabs on the left side of the dialog box appear.
 - b. Click the **ID Info** tab.
 - c. Uncheck the **In Domino Directory** check box.



Caution If you save the ID file in the Domino directory, regardless of whether you also save it in a file, Cisco Unity will not function properly.

- d. Check the **In File** check box.
- e. Choose a location for the ID file, and make note of where you saved it. You will use it when you configure Lotus Notes on the Cisco Unity server, later in the installation.

- Step 3** Add the Cisco Unity Person to the **UnityServers** group that you created in [Step 1](#). Refer to the applicable IBM Lotus documentation.
- Step 4** In the Access Control List for Admin4.nsf, grant the UnityServers group **Editor** permissions.
- Step 5** In the Access Control List for Names.nsf, grant the UnityServers group **Editor with Delete Documents** permissions.
- Step 6** On the Security tab of the Server document of the Domino address book server, grant the UnityServers group the permission to **Create Databases and Templates**. (You will specify the Domino server to use as the address book server during Cisco Unity installation in the Cisco Unity Message Store Configuration wizard.)
- Step 7** Install **csServer**, the server component of DUC for Cisco, on the following servers:
- On each Domino server that will home Cisco Unity subscribers.
 - On the Domino server on which you created the Lotus Notes mail file in [Step 2](#).



Caution Do not install csServer on the Cisco Unity server.

- Step 8** If you selected the mail template MailX.ntf (where X is the version of Domino in use—for example, Mail6.ntf for Domino 6.0) during csServer installation in [Step 7](#), skip to [Step 9](#).
- If you selected a mail template other than MailX.ntf (where X is the version of Domino in use—for example, Mail6.ntf for Domino 6.0) during csServer installation in [Step 7](#), rerun csServer installation on the Domino server that you intend to use as the address book server for Cisco Unity. (The address book server is the Domino server that Cisco Unity monitors for changes to the primary address book, and the server on which it creates default objects.) Select the option to DUC-enable multiple mail templates, then select the applicable MailX.ntf file.



Caution If you do not DUC-enable the MailX.ntf template, default objects created by Cisco Unity, such as the Unity Messaging account, may not function correctly.

- Step 9** In the Domino Administrator or Lotus Notes client on the server you would typically use to administer the Domino Directory, switch to a Notes ID that has Designer or higher access to the administration server for the Domino Directory, then close all windows applications including the Domino Administrator and Lotus Notes client.



Note The switch is required for the next step. After you begin the step, you cannot switch to another Notes ID.

- Step 10** Install **csAdmin**, the administration component of DUC for Cisco, to update the Domino domain directory database. The database is usually called Names.nsf, but it may have a different name on your system. You install csAdmin only once for the domain. For more detailed installation instructions, refer to the applicable IBM Lotus documentation.



Caution Do not install csAdmin on the Cisco Unity server.

- Step 11** Confirm that the network is configured so that Cisco Unity can resolve the unqualified Domino server name to an IP address. (For example, if the Domino server name is MailServer and you enter ping mailserver on the command line on the Cisco Unity server, the response is the IP address of the Domino server.)

Installing and Configuring Lotus Notes on the Cisco Unity Server

You install Notes on the Cisco Unity server because Cisco Unity communicates with Domino by using the Notes software.

You can also use Notes for troubleshooting (for example, to determine whether messages are getting from the Cisco Unity server to Domino users), but you must stop Cisco Unity before you start Notes. When you are finished troubleshooting, exit the Notes software, and shut down and restart the Cisco Unity server.



Caution

Do not run Notes on the Cisco Unity server while Cisco Unity is running, or Cisco Unity may stop functioning.



Caution

Do not install an unsupported version of Notes on the Cisco Unity server. For a list of Notes versions supported on the Cisco Unity server, refer to the applicable *System Requirements for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.



Caution

Do not install csClient or csiNotes, the client component of DUC for Cisco, on the Cisco Unity server.

Do the following three procedures in the order listed.

To Install Lotus Notes on the Cisco Unity Server

- Step 1** On the Cisco Unity server, insert the IBM Lotus Notes disc in the DVD drive.
- Step 2** Browse to the **Lotus Notes** directory, and double-click **Setup.exe**.
- Step 3** Follow the on-screen prompts, and accept the default settings until you are prompted to enter a user name and organization.
- Step 4** Enter a user name and organization, and click **Only for Me**.
- Step 5** Click **Next**.
- Step 6** When you are prompted to specify destination folders, for both the program and the data folders, use the drive location for binary files that you made note of in the “[Determining the Locations for Files on the Cisco Unity Server](#)” section on page 2-4.
- Make note of the drive and directory for the program folder because you will need this information for the next procedure.
- Step 7** Click **Next**.
- Step 8** Follow the on-screen prompts, and accept the default settings.

- Step 9** If a dialog window appears warning about a read-only file that is about to be replaced, check the **Don't Display Again** check box, and click **No**.
- Step 10** Click **Finish**.
-

To Add the Location of the Lotus Notes Program Folder to the System Path Environment Variable

- Step 1** Right-click the **My Computer** icon on the Windows desktop, and click **Properties**.
- Step 2** Click the **Advanced** tab.
- Step 3** Click **Environment Variables**.
- Step 4** In the System Variables list, click **Path**, and click **Edit**.
- Step 5** In the Edit System Variable dialog box, at the end of the **Variable Value** field, enter a semicolon (;) and the drive and directory of the Lotus Notes program folder.
- Step 6** Click **OK** to close the Edit System Variable dialog box.
- Step 7** Click **OK** to close the Environment Variables dialog box.
- Step 8** Click **OK** to close the System Properties dialog box.
-

To Configure Lotus Notes to Use the Cisco Unity Account

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Lotus Applications > Lotus Notes**.
- Step 2** On the Welcome screen, click **Next**.
- Step 3** On the User Information screen, enter a user name and the name of the Domino server on which the Cisco Unity mail file was created.
- Step 4** Check the **I Want to Connect to a Domino Server** check box.
- Step 5** Click **Next**.
- Step 6** Browse to the location where you saved the user ID file in the [“To Prepare the Domino Server\(s\) for Cisco Unity” procedure on page 6-2](#), and double-click the file.
- Step 7** Click **Yes** to copy the user ID file for the Cisco Unity user locally, and click **Next**.



Caution If you do not copy the user ID file to the Cisco Unity server, Cisco Unity will not function correctly.

- Step 8** If the Enter Password dialog box appears, enter the password for the Cisco Unity account.
- Step 9** To complete the configuration, follow the on-screen prompts and accept the default values.
- Step 10** Exit Lotus Notes.
-



CHAPTER 7

Creating Accounts for the Installation and Granting Permissions

In this chapter, you do the following tasks in the order listed:

1. Familiarize yourself with the domain accounts you will create in Task 2. See the [“About the Accounts Required for the Cisco Unity Installation”](#) section on page 7-1.
2. Create the applicable domain accounts that are needed to install Cisco Unity. See the [“Creating the Accounts Required for the Cisco Unity Installation”](#) section on page 7-2.
3. *If you created a Cisco Unity administration account in Task 2.:* Add the account either to the local Administrators group—when the Cisco Unity server is a member server—or to the Domain Admins group—when the Cisco Unity server is a domain controller. See the [“Adding the Cisco Unity Administration Account to an Admins Group”](#) section on page 7-3.
4. Set rights and permissions for the accounts that you created in Task 2. See the [“Granting Permissions with the Cisco Unity Permissions Wizard”](#) section on page 7-4.

When you are finished with this chapter, return to [Chapter 1, “Overview of Mandatory Tasks for Installing Cisco Unity”](#) to continue installing the Cisco Unity system.



Note

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

About the Accounts Required for the Cisco Unity Installation

This section describes the following domain accounts that are needed for the Cisco Unity installation:

- [The Account Used to Install Cisco Unity, page 7-2](#)
- [The Account Used to Access the Cisco Unity Administrator, page 7-2](#)
- [The Accounts That Cisco Unity Services Log On As, page 7-2](#)



Note

The same accounts are required for installing a new Cisco Unity 5.0(x) system and for upgrading from previous versions of Cisco Unity.

The Account Used to Install Cisco Unity

If you are installing more than one Cisco Unity server in a site, you can use the same account to install Cisco Unity software on all of the servers.

The Account Used to Access the Cisco Unity Administrator

When you install Cisco Unity, you are prompted to choose the Active Directory domain account that you want to use to access the Cisco Unity Administrator (the website used to perform most administration tasks). During installation, the account is automatically associated with a Cisco Unity subscriber whose class of service allows Cisco Unity Administrator access. (Later you can create additional Cisco Unity subscribers who also can access the Cisco Unity Administrator.)

By default, the Cisco Unity administration account is the installation account. If you prefer to use an account other than the installation account to be the first Cisco Unity administration account, create an additional domain account for that purpose.

When the Cisco Unity server is a domain controller, the Cisco Unity administration account must be a member of the Domain Admins group. When the Cisco Unity server is a member server, the Cisco Unity administration account must be a member of the local Administrators group. Procedures later in this chapter explain how to add the account to the applicable group.

The Accounts That Cisco Unity Services Log On As

During Cisco Unity installation, you are prompted to choose two domain accounts that Cisco Unity services log on as:

- The account that Cisco Unity directory and message store services log on as. Directory services keep subscriber data in the directory synchronized with subscriber data in the Cisco Unity SQL Server database. Message store services allow subscribers to send and receive voice messages by using the telephone user interface.
- The account that local services log on as. By default, local Cisco Unity services log on as the Local System account. We recommend that you not change this.

Creating the Accounts Required for the Cisco Unity Installation

The procedure in this section requires Active Directory Users and Computers (ADUC). If the Cisco Unity server is a domain controller, ADUC is already installed. If ADUC is not installed, do one of the following:

- Install ADUC on the Cisco Unity server. For information, refer to Windows Help.
- In the domain that includes the Cisco Unity server, go to a computer (for example, the domain controller) on which Active Directory Users and Computers is already installed.

To Create Domain Accounts for Cisco Unity Installation, Administration, and Services

-
- Step 1** On the Cisco Unity server or another server where Active Directory Users and Computers is installed, log on to Windows by using an account that is a member of the Domain Admins group.

- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Active Directory Users and Computers**.
- Step 3** In the left pane, expand the domain, right-click **Users** or the organizational unit where you want to create the installation account, and click **New > User**.
- Step 4** Follow the on-screen prompts to create the installation account.
We suggest that you use the following names for the accounts:

Installation	UnityInstall
Administration	UnityAdmin
Account that Cisco Unity directory and message store services log on as	UnitySvc

- Step 5** Repeat [Step 3](#) and [Step 4](#) to create the Cisco Unity administration account and the account that Cisco Unity directory and message store services log on as.
For the account that Cisco Unity directory and message store services log on as, ensure that the password for the account will never expire. If the password expires, Cisco Unity will stop working the next time the server is restarted.
- Step 6** Close Active Directory Users and Computers.

Adding the Cisco Unity Administration Account to an Admins Group



Note

If you did not create a Cisco Unity administration account in the [“Creating the Accounts Required for the Cisco Unity Installation”](#) section on page 7-2, skip this section.

You must add the Cisco Unity administration account either to the local Administrators group—when the Cisco Unity server is a member server—or to the Domain Admins group—when the Cisco Unity server is a domain controller.

This section contains two procedures. Do the one that applies to your installation.

To Add the Cisco Unity Administration Account to the Local Administrators Group (Only When the Cisco Unity Server Is a Member Server)

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Computer Management**.
- Step 2** In the left pane of the Computer Management MMC, expand **System Tools > Local Users and Groups**.
- Step 3** In the left pane, click **Groups**.
- Step 4** In the right pane, double-click **Administrators**.
- Step 5** In the Administrators Properties dialog box, click **Add**.
- Step 6** In the Select Users or Groups dialog box, in the Look In list, click the name of the domain to which the Cisco Unity server belongs.

- Step 7** In the top list, double-click the name of the Cisco Unity administration account. The name appears in the bottom list.
- Step 8** Click **OK** to close the Select Users or Groups dialog box.
- Step 9** Click **OK** to close the Administrators Properties dialog box.
- Step 10** Close the Computer Management MMC.

To Add the Cisco Unity Administration Account to the Domain Admins Group (Only When the Cisco Unity Server Is a Domain Controller)

- Step 1** On the Cisco Unity server or another server where Active Directory Users and Computers is installed, log on to Windows by using an account that is a member of the Domain Admins group.
 - Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Active Directory Users and Computers**.
 - Step 3** In the left pane, expand the domain, and click **Users**.
 - Step 4** In the right pane, double-click the name of the Cisco Unity administration account.
 - Step 5** Click the **Member Of** tab.
 - Step 6** Click **Add**.
 - Step 7** In the Select Groups dialog box, in the top list, double-click **Domain Admins**. The name appears in the bottom list.
 - Step 8** Click **OK** to close the Select Groups dialog box.
 - Step 9** Click **OK** to close the Properties dialog box.
-

Granting Permissions with the Cisco Unity Permissions Wizard

The Cisco Unity Permissions wizard is frequently updated between Cisco Unity releases. We recommend that you download and run the latest version of the Permissions wizard that is applicable to your version of Cisco Unity. The Permissions wizard is available at http://www.ciscounitytools.com/4_x_tools.htm.

For information on granting permissions with the Permissions wizard, refer to the Permissions wizard Help file PWHelp_<language>.htm that is included with the version of the Permissions wizard that you are using.



Caution

If you are running the Permissions Wizard by using Windows Terminal Services (WTS), the PWDiag.Log file will be deleted at the end of the WTS session. To save it, you must copy it to another location before you end the session.

For a complete list of the permissions set by the Permissions wizard, refer to the Permissions wizard Help file PWHelpPermissionsSet_<language>.htm.



CHAPTER 8

Installing and Configuring Cisco Unity Software

In this chapter, you do the following tasks in the order listed:

1. Determine whether to set up Cisco Unity to use SSL. See the [“Determining Whether to Set Up Cisco Unity to Use SSL”](#) section on page 8-2.
2. *If you plan to set up Cisco Unity to use SSL and want to use the Microsoft Certificate Services available with Windows to issue your own certificate:* Install the Microsoft Certificate Services component. See the [“Installing the Microsoft Certificate Services Component”](#) section on page 8-2.
3. Use the Cisco Unity Installation and Configuration Assistant to install and configure Cisco Unity, and to set up the Cisco Personal Communications Assistant to use SSL. See the [“Installing and Configuring Cisco Unity Software”](#) section on page 8-3.
4. Test the phone system integration. See the [“Testing the Phone System Integration”](#) section on page 8-14.
5. *If virus-scanning software is installed on the Cisco Unity server:* Exclude selected directories from scanning. See the [“Excluding Selected Directories from Virus Scanning”](#) section on page 8-14.
6. Delete Apache Tomcat sample directories. See the [“Deleting Apache Tomcat Sample Directories”](#) section on page 8-14.
7. *If you are setting up Cisco Unity to use SSL:* Set up the Cisco Unity Administrator and Status Monitor to use SSL. See the [“Setting Up the Cisco Unity Administrator and Status Monitor to Use SSL”](#) section on page 8-15.
8. *If Windows Server 2003 is installed on the Cisco Unity server:* Configure Internet Explorer. See the [“Configuring Internet Explorer to Display the Cisco Unity Administrator Correctly \(Windows Server 2003 Only\)”](#) section on page 8-17.
9. Secure the Example Administrator account against toll fraud. See the [“Securing the Example Administrator Account Against Toll Fraud”](#) section on page 8-18.
10. Move SQL Server or MSDE databases and transaction logs. See the [“Moving the Data Store Databases and Transaction Logs”](#) section on page 8-19.
11. Install the latest Microsoft service packs qualified for use with Cisco Unity, if any. In addition, run the latest Cisco Unity Server Updates wizard to install the latest updates recommended for use with Cisco Unity. See the [“Installing the Latest Microsoft Service Packs and Updates”](#) section on page 8-21.
12. *If virus-scanning software or Cisco Security Agent for Cisco Unity is installed on the Cisco Unity server:* Re-enable virus-scanning services and the Cisco Security Agent service for Cisco Unity. See the [“Re-enabling Virus-Scanning and Cisco Security Agent Services”](#) section on page 8-22.

13. If you are running Domino without clustering, consider enabling the Unity Messaging Repository conversation. See the [“Enabling the Unity Messaging Repository Conversation”](#) section on page 8-22.
14. Secure Cisco Unity and the Cisco Unity server. See the [“Securing Cisco Unity and the Cisco Unity Server”](#) section on page 8-23.

When you are finished with this chapter, return to [Chapter 1, “Overview of Mandatory Tasks for Installing Cisco Unity”](#) to continue installing the Cisco Unity system.

**Note**

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Determining Whether to Set Up Cisco Unity to Use SSL

When subscribers log on to the Cisco Personal Communications Assistant (PCA), their credentials are sent across the network to Cisco Unity in clear text. The same is true when the Cisco Unity Administrator and the Status Monitor are configured to use the Anonymous authentication method. In addition, the information that subscribers enter on the pages of the Cisco PCA and of the Cisco Unity Administrator (regardless of which authentication method it uses) is not encrypted.

For increased security, we recommend that you set up Cisco Unity to use the Secure Sockets Layer (SSL) protocol. SSL uses public/private key encryption to provide a secure connection between servers and clients, and uses digital certificates to authenticate servers or servers and clients. (A digital certificate is a file that contains encrypted data that attests to the identity of an organization or entity, such as a computer.)

Using the SSL protocol ensures that all Cisco Unity subscriber credentials—as well as the information that a subscriber enters on any page of the Cisco Unity Administrator and the Cisco PCA—are encrypted as the data is sent across the network. In addition, when you set up Cisco Unity to use SSL, each time that a subscriber tries to access any Cisco Unity web application, the browser will confirm that it is connected with the real Cisco Unity server—and not an entity falsely posing as such—before allowing the subscriber to log on.

To set up a web server such as Cisco Unity to use SSL, you can either obtain a digital certificate from a certificate authority (CA) or use Microsoft Certificate Services available with Windows to issue your own certificate. (A CA is a trusted organization or entity that issues and manages certificates at the request of another organization or entity.) Cost, certificate features, ease of setup and maintenance, and the security policies practiced by the organization are some of the issues to consider when determining whether you should purchase a certificate from a CA or issue your own.

Information on third-party CAs, Microsoft Certificate Services, and SSL is widely available on the Internet, as well as in the Windows and IIS online documentation. Such sources can help you determine whether to use SSL and how to set up a web server to use it.

Installing the Microsoft Certificate Services Component

**Note**

If you do not plan to set up Cisco Unity to use SSL or if you want to use a digital certificate from a certificate authority to set up Cisco Unity to use SSL, skip this section.

Do the procedure in this section if you plan to set up Cisco Unity to use SSL and you want to use the Microsoft Certificate Services available with Windows to issue your own certificate. You may install the component on the Cisco Unity server or on another server.

To Install the Microsoft Certificate Services Component

-
- Step 1** On the server that will act as your certificate authority (CA) and issue certificates, on the Windows Start menu, click **Settings > Control Panel > Add/Remove Programs**.
- Step 2** Click **Add/Remove Windows Components**.
- Step 3** In the Windows Components dialog box, check the **Certificate Services** check box. Do not change any other items. When the warning appears about not being able to rename the computer, or to join or be removed from a domain, click **Yes**.
- Step 4** Click **Next**.
- Step 5** Click **Stand-alone Root CA**, and click **Next**. (A stand-alone CA is a CA that does not require Active Directory.)
- Step 6** Follow the on-screen prompts to complete the installation. For information, refer to the Windows documentation.
- If a message appears that Internet Information Services is running on the computer and must be stopped before proceeding, click **OK** to stop the services.
- Step 7** In the Completing the Windows Components Wizard dialog box, click **Finish**.
- Step 8** Close the Add Remove Programs dialog box and Control Panel.
-

Installing and Configuring Cisco Unity Software

To install and configure Cisco Unity software, you use the Cisco Unity Installation and Configuration Assistant to run seven programs in a specific order. The programs:

- Check the system and install the Cisco Unity software.
- Install the Cisco Unity licenses.
- Configure the Cisco Unity services.
- Configure Cisco Unity for the message store.
- Set new default passwords for the Default Administrator and the Default Subscriber templates
- Integrate Cisco Unity with the phone system.
- Configure the Cisco Personal Communications Assistant to use SSL.

Do the following seven subsections in the order listed.

Starting the Cisco Unity Installation and Configuration Assistant and Installing Cisco Unity Software

From the Cisco Unity Installation and Configuration Assistant, you run the Cisco Unity Setup program first to install Cisco Unity. The Setup program checks the system, then installs the Cisco Unity software.

**Caution**

Do not install Cisco Unity remotely by using Windows Terminal Services or other remote-access applications, or the installation may fail.

**Caution**

Do not install features for which the system is not licensed, or Cisco Unity will shut down.

To Start the Assistant and Install the Cisco Unity Software

Step 1 Log on to Windows by using the Cisco Unity installation account.

**Caution**

If you have not already done so, disable virus-scanning and Cisco Security Agent services on the server, if applicable. Otherwise, the installation may fail.

Step 2 On Cisco Unity DVD 1, browse to the root directory and double-click **Setup.exe**.

Step 3 Follow the on-screen prompts until the Install Cisco Unity page appears.

Step 4 Click **Run the Cisco Unity Setup Program**.

Step 5 Follow the on-screen prompts until the Enter Installation Locations page appears.

Step 6 Specify locations for the Cisco Unity application, trace logs, and Unity Messaging Repository (UMR) files. Use the locations you made note of in the [“Determining the Locations for Files on the Cisco Unity Server”](#) section on page 2-4.

Step 7 Click **Next**.

Step 8 In the Select Features dialog box:

- a. Check the **Install Cisco Unity** check box.
- b. If the Cisco Unity license includes text to speech, check the **Enable TTS** check box.
If not, uncheck the **Enable TTS** check box.
- c. If the Cisco Unity server or an attached expansion chassis contains Intel Dialogic voice cards, check the **Install Voice Card Software** check box.
If not, uncheck the **Install Voice Card Software** check box.

**Note**

If Windows Server 2003 is installed on the Cisco Unity server, the Install Voice Card Software check box is not available. Circuit-switched phone system integrations that use voice cards are not supported with a Cisco Unity server on which Windows Server 2003 is installed.

Step 9 Click **Next**.

Step 10 Choose the prompt set to install. Consider the following:

- Cisco Unity should use the same audio format for prompts that the phone system uses for the media stream. Using a consistent audio format minimizes the need for transcoding from one audio format to another and minimizes the performance impact on the Cisco Unity server.
- Callers hear consistent sound quality when the prompts are in the same audio format that is used for recording messages.
- The G.711 Mu-Law audio format offers superior audio quality.

- The G.729a audio format uses less network bandwidth.

Note that choosing a system prompt set does not change the default message recording and storage codec. If necessary, you can change the message recording and storage codec after Cisco Unity is installed.

Step 11 Click **Next**.

Step 12 In the Cisco Unity Languages dialog box, choose the language(s) to install, and click **Next**.

If you installed Windows by using the manufacturer's guided system-setup utility and a retail Windows disc, one of the languages you choose here must match the locale you specified when you installed Windows.



Caution

If the locale you specified when you installed Windows does not match any of the installed Cisco Unity system-prompt languages, Cisco Unity will log errors in the event log and may stop taking calls. The system-prompt language you choose here must exactly match the locale you selected when you installed Windows. For example, if you chose English (United Kingdom) for locale, you must also choose English (United Kingdom) as one of the Cisco Unity system-prompt languages. English (Australia) will not work.

If you installed Windows by using the Platform Configuration discs that are shipped with the Cisco Unity server, the locale is automatically set to English (United States). The Cisco Unity Setup program always installs English (United States) system prompts, so you do not need to choose it as one of the languages to install.


Note that if the system will be using text to speech (TTS) and will be using English (Australia) or English (New Zealand) for the system prompts, also install English (United States) or English (United Kingdom) for the TTS language.

Step 13 Set the system-default languages for the phone, graphical user interface (GUI), and TTS, and click **Next**.

For the phone (system prompts) language, choose the language that matches the locale that you specified when you installed Windows.

Step 14 Follow the on-screen prompts until you are prompted to restart the Cisco Unity server.

- Step 15** The remainder of the procedure depends on whether the server contains Intel Dialogic D/120JCT-Euro or D/240PCI-T1 voice cards:

If the server does not contain Intel Dialogic D/120JCT-EURO or D/240PCI-T1 voice cards	Check the Yes, I Want to Restart My Computer Now check box, and click Finish . Cisco Unity software is now installed.
If the server contains Intel Dialogic D/120JCT-EURO or D/240PCI-T1 voice cards	<p>a. Uncheck the Yes, I Want to Restart My Computer Now check box, and click Finish.</p> <p> Caution If the Cisco Unity server contains Intel Dialogic D/120JCT-EURO or D/240PCI-T1 voice cards, do not restart the server now or you will not be able to access the Cisco Unity Administrator after Cisco Unity is installed.</p> <p>b. Do the procedure under “Software Settings” for your voice card in Appendix A, “Voice Cards and PIMG Units.”</p> <p>c. Restart the Cisco Unity server.</p>

Installing License Files

From the Cisco Unity Installation and Configuration Assistant, you run the Cisco Unity Install License File wizard second to install the Cisco Unity license files.

To Install the License Files

- Step 1** Log on to Windows by using the Cisco Unity installation account.
- Step 2** On the Install the Cisco Unity License Files page, click **Run the Cisco Unity Install License File Wizard**.
- Step 3** On the Welcome page, click **Next**.
- Step 4** Click **Add**.
- Step 5** Insert the Cisco Unity license file disk, if applicable.
- (When Cisco Unity was registered on Cisco.com, Cisco replied with an e-mail containing attached file(s) with license(s) for Cisco Unity features. The instructions in the e-mail directed that the attached files be saved. For more information, see the [“Obtaining Cisco Unity License Files”](#) section on page 5-4.)
- Step 6** Browse to drive A or to the location where the license file(s) have been stored.
- Step 7** Double-click the license file to add it to the License Files list.
- If prompted, click **Yes** to copy the license file to the local system.
- Step 8** If you are adding more than one license file, click **Add**, and repeat [Step 6](#) and [Step 7](#) for each license file.
- Step 9** Click **Next**.
- Step 10** In the Licenses dialog box, confirm that the license information is correct.

Step 11 Click **Next**.

Step 12 Click **Finish**.

When the wizard is complete, the Configure the Cisco Unity Services page appears in the main window.

Configuring Services

From the Cisco Unity Installation and Configuration Assistant, you run the Cisco Unity Services Configuration wizard third to associate the directory, message store, and local services with accounts you specify.

To Configure Services

Step 1 On the Configure the Cisco Unity Services page, click **Run the Cisco Unity Services Configuration Wizard**. (Note that you should be logged on to Windows with the Cisco Unity installation account.)

Step 2 On the Welcome page, click **Next**.

Step 3 Click **Lotus Domino**.

Step 4 Click **Next**.

Step 5 Follow the on-screen prompts to complete the configuration.

When the wizard is complete, the Configure the Cisco Unity Message Store page appears in the main window.

Configuring Cisco Unity for the Message Store

From the Cisco Unity Installation and Configuration Assistant, you run the Cisco Unity Message Store Configuration wizard fourth to configure Cisco Unity for the message store.

To Configure Cisco Unity for the Message Store

Step 1 On the Configure the Cisco Unity Message Store page, click **Run the Cisco Unity Message Store Configuration Wizard**. (Note that you should be logged on to Windows with the Cisco Unity installation account.)

Step 2 Confirm that the Domino server is running. If Domino is not running, configuring the message store on the Cisco Unity server will fail.

Step 3 Follow the on-screen prompts until the Primary Address Book Information page appears.

In the following fields, enter information for the directory database that you will use to import subscribers and public distribution lists:

Server Name	The Domino name for the server. This name must be resolvable to an IP address by using DNS, a HOSTS file, or some other mechanism. If you re-ran the csServer installation to DUC-enable the MailX.ntf template in Step 8 of the “ To Prepare the Domino Server(s) for Cisco Unity ” procedure on page 6-2, the server that you specify here must be the server on which you re-ran csServer. If you decide to use a different Domino server, or if you are unsure whether you re-ran csServer on the correct server, repeat the step on the correct server before continuing with this procedure.
Address Book	The name of the Domino directory database. Typically, this is Names.nsf, unless you are using a different name for your Domino directory database.
Display Name	The Cisco Unity Administrator uses the text name you enter here for the file you entered in the Address Book field.

- Step 4** Follow the on-screen prompts to complete the wizard.
When the wizard is complete, the Set New Default Passwords page appears in the main window.

Setting New Default Passwords

From the Cisco Unity Installation and Configuration Assistant, you run the Password Hardening wizard fifth to set new default passwords for the Default Administrator and the Default Subscriber templates.

To Set New Default Passwords

- Step 1** On the Set New Default Passwords page, click **Run the Password Hardening Wizard**.
- Step 2** Follow the on-screen prompts.
When the Password Hardening wizard finishes, the Integrate the Phone System with Cisco Unity page appears in the main window.

Integrating the Phone System with Cisco Unity

From the Cisco Unity Installation and Configuration Assistant, you run the Cisco Unity Telephony Integration Manager (UTIM) sixth to connect Cisco Unity with the phone system.

To Integrate the Phone System with Cisco Unity

- Step 1** On the Integrate the Phone System with Cisco Unity page, click **Run the Cisco Unity Telephony Integration Manager**. (Note that you should be logged on to Windows with the Cisco Unity installation account.)
- Step 2** In the right pane of the UTIM, click **Create Integration**.

Step 3 Refer to the applicable Cisco Unity integration guide for your phone system to complete the integration. (Cisco Unity integration guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.)

When the integration is complete, the Set Up the Cisco Personal Communications Assistant to Use SSL page appears in the main window.

Setting Up the Cisco Personal Communications Assistant to Use SSL

From the Cisco Unity Installation and Configuration Assistant, you can set up the Cisco PCA to use SSL. Using the SSL protocol ensures that all subscriber credentials—as well as the information that a subscriber enters on any page in the Cisco PCA—are encrypted as the data is sent across the network.

After the Cisco Unity Installation and Configuration Assistant is finished and the Cisco PCA is set up to use SSL, you manually set up the Cisco Unity Administrator and Status Monitor to use SSL. The *Cisco Unity Installation Guide* alerts you when to do the procedure.

If you do not want to set up the Cisco PCA to use SSL, see the “[Skipping Cisco PCA Setup for SSL](#)” section on page 8-9.

To set up the Cisco PCA to use SSL, do the procedures in the applicable section, depending on whether you are using a certificate authority:

- [Setting Up the Cisco PCA to Use SSL by Creating a Local Certificate Without a Certificate Authority](#), page 8-10
- [Setting Up the Cisco PCA to Use SSL by Using a Certificate Authority](#), page 8-11

If the Cisco Unity server is running Windows Server 2003, you can set up the Cisco Personal Communications Assistant to use SSL now. However, the option to do so by creating a local certificate without a certificate authority has not been automated for Windows Server 2003. If you want to set up the Cisco PCA to use SSL by using this method, you must do so manually. Refer to the online help available on this page.

Skipping Cisco PCA Setup for SSL

Do the procedure in this section if you do not want to set up the Cisco PCA to use SSL. (Note that without SSL when subscribers log on to the Cisco PCA, their credentials will be sent across the network to Cisco Unity in clear text. In addition, the information that subscribers enter on the pages of the Cisco PCA will not be encrypted.)

To Skip Cisco PCA Setup for SSL

- Step 1** On the Set Up the Cisco Personal Communications Assistant to Use SSL page, Click **Do Not Set Up Cisco Personal Communications Assistant to Use SSL**.
- Step 2** Click **Continue**.
- Step 3** Click **Close** to exit the Cisco Unity Installation and Configuration Assistant.
-

Setting Up the Cisco PCA to Use SSL by Creating a Local Certificate Without a Certificate Authority

To Set Up the Cisco PCA to Use SSL by Creating a Local Certificate Without a Certificate Authority

-
- Step 1** On the Set Up the Cisco Personal Communications Assistant to Use SSL page, click **Create a Local Certificate Without a Certificate Authority**.
 - Step 2** Click **Internet Services Manager**.
 - Step 3** Expand the name of the Cisco Unity server.
 - Step 4** Right-click **Default Web Site**, and click **Properties**.
 - Step 5** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
 - Step 6** Under Secure Communications, click **Server Certificate**.
 - Step 7** On the Web Server Certificate wizard Welcome page, click **Next**.
 - Step 8** Click **Create a New Certificate**, and click **Next**.
 - Step 9** Click **Prepare the Request Now, But Send It Later**, and click **Next**.
 - Step 10** Enter a name and a bit length for the certificate.

We strongly recommend that you choose a bit length of 512. Greater bit lengths may decrease performance.

- Step 11** Click **Next**.
- Step 12** Enter the organization information, and click **Next**.
- Step 13** For the common name of the site, enter either the system name of the Cisco Unity server or the fully qualified domain name.



Caution The name must exactly match the host portion of any URL that will access the system by using a secure connection.

- Step 14** Click **Next**.
- Step 15** Enter the geographical information, and click **Next**.
- Step 16** Specify the certificate request file name and location, and write down the file name and location because you will need the information later in this procedure.
- Step 17** Click **Next**.
- Step 18** Verify the request file information, and click **Next**.
- Step 19** Click **Finish** to exit the Web Server Certificate wizard.
- Step 20** Click **OK** to Close the Default Web Site Properties dialog box.
- Step 21** Close the Internet Services Manager window.
- Step 22** In the Cisco Unity Installation and Configuration Assistant, in the Enter Certificate Request File box, enter the full path and file name of the certificate request file that you specified in [Step 16](#).
- Step 23** Click **Create Certificate**.
- Step 24** Click **Internet Services Manager**.
- Step 25** Expand the name of the Cisco Unity server.
- Step 26** Right-click **Default Web Site**, and click **Properties**.

- Step 27** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
 - Step 28** Under Secure Communications, click **Server Certificate**.
 - Step 29** On the Web Server Certificate wizard Welcome page, click **Next**.
 - Step 30** Click **Process the Pending Request and Install the Certificate**.
 - Step 31** Click **OK**.
 - Step 32** In the Process a Pending Request dialog box, click **OK** to accept the default path and file name of the pending certificate request.
 - Step 33** In the Certificate Summary dialog box, click **Next**.
 - Step 34** Click **Finish** to exit the Web Server Certificate wizard.
 - Step 35** Click **OK** to Close the Default Web Site Properties dialog box.
 - Step 36** Close the Internet Services Manager window.
 - Step 37** In the Cisco Unity Installation and Configuration Assistant, click **Enable Cisco PCA to Use SSL**.
 - Step 38** Click **Internet Services Manager**.
 - Step 39** Right-click the name of the Cisco Unity server, and click **Restart IIS**.
 - Step 40** In the Stop/Start/Restart dialog box, click **Restart Internet Services on <Servername>**.
 - Step 41** Click **OK**.
 - Step 42** Close the Internet Services Manager window.
 - Step 43** In the Cisco Unity Installation and Configuration Assistant, click **Continue**.
 - Step 44** Click **Close** to exit the Cisco Unity Installation and Configuration Assistant.
-

Setting Up the Cisco PCA to Use SSL by Using a Certificate Authority

This section contains four procedures.

If you are using Microsoft Certificate Services to issue your own certificate, do all four procedures in the order listed.

If you are using a certificate purchased from a certificate authority (for example, VeriSign), do only the fourth procedure, “[To Install the Certificate](#).”

To Create a Certificate Request by Using Microsoft Certificate Services

- Step 1** On the Set Up the Cisco Personal Communications Assistant to Use SSL page, click **Use a Certificate Authority**.
- Step 2** Click **Internet Services Manager**.
- Step 3** Expand the name of the Cisco Unity server.
- Step 4** Right-click **Default Web Site**, and click **Properties**.
- Step 5** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 6** Under Secure Communications, click **Server Certificate**.
- Step 7** On the Web Server Certificate wizard Welcome page, click **Next**.
- Step 8** Click **Create a New Certificate**, and click **Next**.

- Step 9** Click **Prepare the Request Now, But Send It Later**, and click **Next**.
- Step 10** Enter a name and a bit length for the certificate.
We strongly recommend that you choose a bit length of 512. Greater bit lengths may decrease performance.
- Step 11** Click **Next**.
- Step 12** Enter the organization information, and click **Next**.
- Step 13** For the common name of the site, enter either the system name of the Cisco Unity server or the fully qualified domain name.



Caution The name must exactly match the host portion of any URL that will access the system by using a secure connection.

- Step 14** Click **Next**.
- Step 15** Enter the geographical information, and click **Next**.
- Step 16** Specify the certificate request file name and location, and write down the file name and location because you will need the information in the next procedure.
Save the file to a disk or to a directory that the certificate authority (CA) server can access.
- Step 17** Click **Next**.
- Step 18** Verify the request file information, and click **Next**.
- Step 19** Click **Finish** to exit the Web Server Certificate wizard.
- Step 20** Click **OK** to Close the Default Web Site Properties dialog box.
- Step 21** Close the Internet Services Manager window.
- Step 22** Click **Close** to exit the Cisco Unity Installation and Configuration Assistant.

To Submit the Certificate Request by Using Microsoft Certificate Services

- Step 1** On the server that is acting as the CA, on the Windows Start menu, click **Run**.
- Step 2** Run **Certreq**.
- Step 3** Browse to the directory where you saved the certificate request file, and double-click the file.
- Step 4** Click the CA to use, and click **OK**.
-

Once the CA submits the certificate request, it assigns a pending status by default for added security. This requires a person to verify the authenticity of the request and to manually issue the certificate.

To Issue the Certificate by Using Microsoft Certificate Services

- Step 1** On the server that is acting as the CA, on the Windows Start menu, click **Programs > Administrative Tools > Certification Authority**.
- Step 2** In the left pane of the Certification Authority window, expand **Certification Authority**.
- Step 3** Expand <Certification Authority name>.

- Step 4** Click **Pending Requests**.
 - Step 5** In the right pane, right-click the request, and click **All Tasks > Issue**.
 - Step 6** In the left pane, click **Issued Certificates**.
 - Step 7** In the right pane, double-click the certificate to open it.
 - Step 8** Click the **Details** tab.
 - Step 9** In the Show list, choose **<All>**, and click **Copy to File**.
 - Step 10** On the Certificate Export wizard Welcome page, click **Next**.
 - Step 11** Accept the default export file format **DER encoded binary X.509 (.CER)**, and click **Next**.
 - Step 12** Specify a file name and a location that the Cisco Unity server can access, and click **Next**.
 - Step 13** Verify the settings, and click **Finish**.
 - Step 14** Click **OK** to close the Certificate Details dialog box.
 - Step 15** Close the Certification Authority window.
-

To Install the Certificate

- Step 1** On the Cisco Unity server, double-click the **CUICA** icon on the desktop.
- Step 2** In the Cisco Unity Installation and Configuration Assistant, click **Use a Certificate Authority**.
- Step 3** On the Set Up the Cisco Personal Communications Assistant to Use SSL page, at Step 3, click **Internet Services Manager**.
- Step 4** Expand the name of the Cisco Unity server.
- Step 5** Right-click **Default Web Site**, and click **Properties**.
- Step 6** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 7** Under Secure Communications, click **Server Certificate**.
- Step 8** On the Web Server Certificate wizard Welcome page, click **Next**.
- Step 9** Click **Process the Pending Request and Install the Certificate**, and click **Next**.
- Step 10** Browse to the directory of the certificate (.cer) file, and double-click the file.
- Step 11** Verify the certificate information, and click **Next**.
- Step 12** Click **Finish** to exit the Web Server Certificate wizard.
- Step 13** Click **OK** to close the Default Web Site Properties dialog box.
- Step 14** Close the Internet Services Manager window.
- Step 15** In the Cisco Unity Installation and Configuration Assistant, click **Enable Cisco PCA to Use SSL**.
- Step 16** Restart IIS:
 - a. Click **Internet Services Manager**.
 - b. Right-click the name of the Cisco Unity server, and click **Restart IIS**.
 - c. In the Stop/Start/Restart dialog box, click **Restart Internet Services on <Servername>**.

- d. Click **OK**.
- e. Close the Internet Services Manager window.

Step 17 Click **Close** to exit the Cisco Unity Installation and Configuration Assistant.

Testing the Phone System Integration

Test the integration with the phone system. Refer to the Cisco Unity integration guide for your phone system.

Note that you use the Cisco Unity Administrator for part of the integration test. Use the user name and password for the account that you selected to administer Cisco Unity.

Excluding Selected Directories from Virus Scanning

Revised May 1, 2008



Note

If virus-scanning software is not installed on the Cisco Unity server, skip this section.

You exclude selected directories from scanning to improve Cisco Unity performance and reliability.

To Exclude Selected Directories from Virus Scanning

Step 1 Refer to the virus-scanning software Help for instructions on excluding directories from scanning.

Step 2 Exclude the following directories from virus scanning:

- The directory in which Cisco Unity is installed (Commsvr by default), and all subdirectories.
 - The directory that contains the files UnityDB.mdf and UnityDb_log.ldf.
 - The directory specified in the Temp system variable for the directory and message store services account. (To find this directory, log on as the directory and message store services account. Open a command-prompt window, and run the **set temp** command.)
-

Deleting Apache Tomcat Sample Directories

Added May 1, 2008

Apache Tomcat, which is automatically installed on the Cisco Unity server and is required for Cisco Unity to function properly, contains security vulnerabilities in sample applications. To eliminate the security vulnerabilities, do the following procedure to delete the sample directories. For more information, see the CVE-IDs “CVE-2007-1355” and “CVE-2007-2449” on the CVE (Common Vulnerabilities and Exposures) website at <http://cve.mitre.org>.

To Delete Apache Tomcat Sample Applications

- Step 1** In the Services MMC, stop the Tomcat service.
- Step 2** Delete the following directories and their contents under the directory where Cisco Unity is installed (Commserver by default):
- cscoserv\Tomcat\webapps\examples
 - cscoserv\Tomcat\webapps\tomcat-docs
- Step 3** In the Services MMC, restart the Tomcat service.
-

Setting Up the Cisco Unity Administrator and Status Monitor to Use SSL



Note

If you are not setting up Cisco Unity to use SSL, skip this section.

Using the SSL protocol ensures that all subscriber credentials—as well as the information that a subscriber enters on any page in the Cisco Unity Administrator—are encrypted as the data is sent across the network.

To Set Up the Cisco Unity Administrator and Status Monitor to Use SSL

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
- Step 2** Expand the name of the Cisco Unity server.
- Step 3** Expand **Default Web Site**.
- Step 4** Under Default Web Site, right-click **Web**, and click **Properties**.
- Step 5** In the Properties dialog box, set the Web directory to use SSL:
- Click the **Directory Security** tab.
 - Under Secure Communications, click **Edit**.
 - Check the **Require Secure Channel (SSL)** check box.
 - Click **OK** to close the Secure Communications dialog box.
 - Click **OK** to close the Properties dialog box.
- Step 6** Under Default Web Site, right-click **SAWeb**, and click **Properties**.
- Step 7** Repeat [Step 5](#) to set the SAWeb directory to use SSL.
- Step 8** Under Default Web Site, right-click **Status**, and click **Properties**.
- Step 9** Repeat [Step 5](#) to set the Status directory to use SSL.
- Step 10** Under Default Web Site, double-click **AvXml**.
- Step 11** In the right pane, right-click **AvXml.dll**, and click **Properties**.
- Step 12** In the Properties dialog box, click the **File Security** tab.

- Step 13** Under Secure Communications, click **Edit**.
 - Step 14** Check the **Require Secure Channel (SSL)** check box.
 - Step 15** Click **OK** to close the Secure Communications dialog box.
 - Step 16** Click **OK** to close the AvXml.dll Properties dialog box.
 - Step 17** Close the Internet Services Manager window.
-

After you have set up the Cisco Unity Administrator and Status Monitor to use SSL, you must make the following changes so the web applications can be started by using the Cisco Unity tray icon and desktop icons:

- Update the Windows registry to change the default HTTP URL to an HTTPS (secure) URL for the tray icon.
- Change the desktop icons to use HTTPS URLs.

Do the following two procedures to change the URLs to secure URLs.

To Change the Default URL for the Cisco Unity Tray Icon to an HTTPS URL

- Step 1** On the Cisco Unity server, start RegEdit.



Caution Changing the wrong registry key or entering an incorrect value can cause the server to malfunction. Before you edit the registry, confirm that you know how to restore it if a problem occurs. (Refer to the “Restoring” topics in Registry Editor Help.) If you have any questions about changing registry key settings, contact Cisco TAC.

- Step 2** If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.
 - Step 3** Expand the key
HKEY_LOCAL_MACHINE\SOFTWARE\Active Voice\SystemParameters\1.0.
 - Step 4** In the left pane, right-click **1.0**, and click **New > DWORD Value**.
 - Step 5** Name the value **EnforceSSL**.
 - Step 6** In the right pane, double-click **EnforceSSL**.
 - Step 7** Change Value Data to **1**.
 - Step 8** Click **OK** to save the change.
 - Step 9** Close Registry Editor.
 - Step 10** Restart the server.
-

To Change the Desktop Icons to Use HTTPS URLs

- Step 1** On the Cisco Unity server, right-click the **System Administration** desktop icon, and click **Properties**.
- Step 2** Click the **Web Document** tab.
- Step 3** In the URL field, change the “http” portion of the URL to **https**.

- Step 4** Click **OK**.
- Step 5** Right-click the **Status Monitor** desktop icon, and click **Properties**.
- Step 6** Click the **Web Document** tab.
- Step 7** In the URL field, change the “http” portion of the URL to **https**.
- Step 8** Click **OK**.

Configuring Internet Explorer to Display the Cisco Unity Administrator Correctly (Windows Server 2003 Only)



Note

If Windows Server 2003 is not installed on the Cisco Unity server or if you installed Windows Server 2003 using the Cisco Unity Platform Configuration discs, skip this section.

If you created a Cisco Unity administration account as recommended in the [“About the Accounts Required for the Cisco Unity Installation”](#) section on page 7-1, and you log on to Windows by using that account, the changes that the Windows Server 2003 service pack make to the default Internet Explorer security settings cause the Cisco Unity Administrator to display a blank page. Do the following procedure to configure Internet Explorer to display the Cisco Unity Administrator when you log on to Windows by using the administration account.

To Configure Internet Explorer to Display the Cisco Unity Administrator Correctly

- Step 1** Log on to the Cisco Unity server by using the Cisco Unity administration account.
- Step 2** Right click the **Cisco Unity** icon in the system tray, and click **Launch System Admin**.
- Step 3** If you are prompted to provide a user name and password, click **Cancel**.
- Step 4** On the Internet Explorer Tools menu, click **Internet Options**.
- Step 5** Click the **Security** tab.
- Step 6** Under Select a Web Content Zone to Specify Its Security Settings, click the **Trusted Sites** icon.
- Step 7** Click **Sites**.
- Step 8** In the Trusted Sites dialog box, in the Add This Website to the Zone field, enter the applicable value depending on whether the Cisco Unity Administrator is set up to use SSL:

Cisco Unity Administrator is set up to use SSL	Enter https:\\<CiscoUnityServerName>
Cisco Unity Administrator is not set up to use SSL	Enter http:\\<CiscoUnityServerName>

- Step 9** If the Cisco Unity Administrator is set up to use SSL, check the **Require Server Verification (https:) for All Sites in This Zone** check box.
- If the Cisco Unity Administrator is not set up to use SSL, uncheck the **Require Server Verification (https:) for All Sites in This Zone** check box.
- Step 10** Click **Add**.

- Step 11** Click **Close** to close the Trusted Sites dialog box.
- Step 12** On the Security tab, click **Custom Level**.
- Step 13** In the Security Settings dialog box, change the value of the Reset To list to **Low**.
- Step 14** Click **Reset**, and click **Yes** to confirm that you want to change the security settings for this zone.
- Step 15** Click **OK** to close the Security Settings dialog box.
- If the Security Settings dialog box does not close:
- a. Close the dialog box by clicking the **X** in the upper-right corner.
 - b. In the “not responding” message box, click **End Now**. (The “not responding” message box may take a few seconds to appear.)
- Step 16** Restart the Cisco Unity Administrator.
-

Securing the Example Administrator Account Against Toll Fraud

It is possible for a malicious user to dial into Cisco Unity, log on as the Example Administrator by using the default extension and password, and configure Cisco Unity to forward calls to phone numbers for which there are charges or to reconfigure greetings so an operator believes the messaging system is personally accepting collect-call charges. To help secure Cisco Unity against toll fraud, we strongly recommend that you change the phone password for the Example Administrator account after Cisco Unity is installed.

To Change the Password on the Example Administrator Account

- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Subscribers** page.
- Step 2** Click the **Find** icon.
- Step 3** On the Find and Select Subscriber page, click **Find**.
- Step 4** Click **Example Administrator**.
- Step 5** In the left pane, click **Phone Password**.
- Step 6** In the right pane, check the **User Cannot Change Password** check box.
- Step 7** Check the **Password Never Expires** check box.
- Step 8** Under **Reset Phone Password**, enter and confirm a new password by using digits 0 through 9.
- We recommend that you enter a long and nontrivial password; 20 digits or more is desirable. (The minimum length of the password is set on the Subscribers > Account Policy > Phone Password Restrictions page.) In a nontrivial password:
- The digits are not all the same (for example, 9999).
 - The digits are not consecutive (for example, 1234).
 - The password is not the same as the extension assigned to the example account.
 - The password does not spell the name of the example account, the name of the company, the name of the IT manager, or any other obvious words.
- Step 9** Click the **Save** icon.

Step 10 Close the Cisco Unity Administrator.

Moving the Data Store Databases and Transaction Logs

The Cisco Unity data store includes several databases and their corresponding transaction logs. Because the Cisco Unity and Reports databases and their transaction logs are the fastest-growing data store files, you place them on the system in a location that makes optimum use of system storage capacity.

As you do the procedure in this section, if applicable, refer to the drive locations you made note of in the [“Determining the Locations for Files on the Cisco Unity Server”](#) section on page 2-4.

For more information on moving SQL Server or MSDE databases and transaction logs, refer to Microsoft documentation.

To Move the SQL Server or MSDE Databases and Transaction Logs

- Step 1** Stop Cisco Unity. (Right-click the **Cisco Unity** icon in the system tray, then click **Stop Cisco Unity**; if the Cisco Unity icon is not available, browse to the **CommServer** directory and double-click **AvCsTrayStatus.exe**.)
- Step 2** In Task Manager, end the Cisco Unity tray icon process:
- Right-click in an empty space on the taskbar and click **Task Manager**.
 - Click the **Processes** tab.
 - Click the **Image Name** column twice to sort by process name.
 - Click **AvCsTrayStatus**.
 - Click **End Process**.
 - Click **Yes** to confirm.
 - Close **Task Manager**.
- Step 3** Stop the AvCsGateway service:
- On the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - In the right pane, right-click **AvCsGateway**, and click **Stop**.
 - Close the Services MMC.
- Step 4** Detach the ReportDB and UnityDb databases:
- On the Windows Start menu, click **Programs > Microsoft SQL Server > Enterprise Manager**.
 - In the left pane, expand **Microsoft SQL Servers > SQL Server Group > (local) (Windows NT) > Databases**.
 - Right-click **ReportDb**, and click **All Tasks > Detach Database**.
 - If the OK button is unavailable, click **Clear**, and click **OK** to confirm that you want to clear connections.
 - Click **OK** to detach the ReportDB database.
 - Click **OK** to confirm.
 - Repeat Step **c.** through Step **f.** to detach the UnityDb database.

- Step 5** Close SQL Server Enterprise Manager.
- Step 6** In Windows Explorer, create the new directories for Cisco Unity data and for transaction logs on the drive locations you made note of in the “[Determining the Locations for Files on the Cisco Unity Server](#)” section on page 2-4. Use directory names that are easy to remember, for example:

UnityDb.mdf and ReportDb.mdf	<Database destination drive>\<Path>\UnityData
ReportDb_log.ldf and UnityDb_log.ldf	<Log file destination drive>\<Path>\UnityLogs

- Step 7** In Windows Explorer, move UnityDb.mdf and ReportDb.mdf from Program Files\Microsoft SQL Server\MSSQL\Data to the new directory for Cisco Unity databases.
- Step 8** In Windows Explorer, move ReportDb_log.ldf and UnityDb_log.ldf from Program Files\Microsoft SQL Server\MSSQL\Data to the new directory for Cisco Unity transaction logs.
- Step 9** Using OSQL, reattach the databases:



Caution If you put the databases and the transaction log in separate locations, as recommended for most systems, you must use OSQL to reattach the databases because SQL Server Enterprise Manager does not support attaching a database when the corresponding log file is not in the same directory.

- a. On the Windows Start menu, click **Run**.
- b. Run **cmd**.
- c. Start OSQL by entering **OSQL -E** on the command line.



Caution Use **-E**, not **-e**.

- d. Enter **use master** and press **Enter**.
- e. Enter **go** and press **Enter**.
- f. Enter **EXEC sp_attach_db 'UnityDb', '<Database destination drive>\<New database directory path>\UnityDb.mdf', '<Log file destination drive>\<New log file directory path>\UnityDb_log.ldf'** and press **Enter**.
- g. Enter **go** and press **Enter**.

If you specified an invalid path or file name, an error message appears in the command window. Re-run Step f. and Step g. with the correct information.

- h. Enter
EXEC sp_attach_db 'ReportDb', '<Database destination drive>\<New database directory path>\ReportDb.mdf', '<Log file destination drive>\<New log file directory path>\ReportDb_log.ldf'
and press **Enter**.
- i. Enter
go
and press **Enter**.

If you specified an invalid path or file name, an error message appears in the command window. Re-run Step **h.** and Step **i.** with the correct information.

- Step 10** Enter
exit
and press **Enter** to close OSQL.
- Step 11** On the Windows Start menu, click **Programs > Startup > AvCsTrayStatus** to restart the Cisco Unity tray icon.
- Step 12** When the tray icon appears in the Windows taskbar, use it to restart Cisco Unity.
-

Installing the Latest Microsoft Service Packs and Updates

You install the latest Microsoft service packs that has been qualified for use with Cisco Unity, if any, as well as the corresponding updates, to enhance the security of the Cisco Unity server. Do the following procedures.

To Install the Latest Microsoft Service Packs, If Any

- Follow the instructions that you printed or downloaded when you downloaded the service pack.
-

To Install the Latest Microsoft Updates Recommended for Use with Cisco Unity

- Step 1** Insert in the drive the disc that you burned with the latest version of the Cisco Unity Server Updates Wizard.
- Step 2** Run **ServerUpdatesWizard.exe**.
- Step 3** Follow the on-screen prompts to complete the installation of Microsoft updates and, optionally, Cisco Security Agent for Cisco Unity.



Note

If you are accessing the server by using Remote Desktop or a VNC client, and you are installing Cisco Security Agent for Cisco Unity, the Remote Desktop or VNC session will be disconnected when Cisco Security Agent for Cisco Unity restarts the network interface. If the session does not reconnect automatically, reconnect manually to finish the Server Updates wizard.

Step 4 Restart the Cisco Unity server.

Re-enabling Virus-Scanning and Cisco Security Agent Services



Note

If virus-scanning software or Cisco Security Agent for Cisco Unity is not installed on the Cisco Unity server, skip this section.

You re-enable virus-scanning and Cisco Security Agent services now that all of the software installations that could have been affected if the services were running are complete.

To Re-enable and Start Virus-Scanning and Cisco Security Agent Services

- Step 1** Refer to the virus-scanning software documentation to determine the names of the virus-scanning services.
- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 3** Re-enable and start each virus-scanning service and the Cisco Security Agent service:
- a. In the right pane, double-click the service.
 - b. On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.
 - c. Click **Start** to start the service.
 - d. Click **OK** to close the Properties dialog box.
- Step 4** When the services have been re-enabled, close the Services MMC.
-

Enabling the Unity Messaging Repository Conversation

If the Domino servers are not configured in a cluster or if there is only one Domino server, do the procedure in this section to allow subscribers increased access to voice messages during an outage.



Caution

Do not enable the Unity Messaging Repository (UMR) conversation if Domino servers are configured in a cluster. Doing so may cause Cisco Unity to unnecessarily hold messages in the UnityMTA directory and restrict subscriber access to messages stored in the UMR, even though subscriber mail files are available on another Domino server in the cluster.

When a Domino server—or even the entire Domino network—is down, Cisco Unity can answer calls, allow unidentified callers to look up subscriber extensions, and take voice messages. While the e-mail system or network is off line, new voice messages are handled by the Unity Messaging Repository on the Cisco Unity server.

The UMR as a feature consists of the following main parts:

- **UnityMTA**—When callers leave messages for subscribers, the messages are temporarily stored in the UnityMTA directory on the Cisco Unity server. If a problem with the network prevents Cisco Unity from handing off the messages to Domino, the messages remain on the hard disk of the Cisco Unity server until they can be delivered. While Domino is unavailable, callers can still leave messages. When the Domino server or network is back on line, voice messages stored in the UMR are routed to subscriber mailboxes.
- **UMR conversation**—When subscribers log on to Cisco Unity and their mail files are unavailable, the UMR conversation provides limited functionality by allowing subscribers to listen to messages left for them in the UnityMTA directory. The UMR conversation is disabled by default. After a subscriber logs on, if Cisco Unity is unable to access the mail file of the subscriber, Cisco Unity plays the failsafe prompt and hangs up. (“This system is temporarily unable to complete your call. Call again later. Goodbye.”)

To Enable the Unity Messaging Repository Conversation

- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
 - Step 2** In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.
 - Step 3** In the Unity Settings pane, click **Conversation—(Unity Domino only) Enable UMR Conversation**.
 - Step 4** In the New Value box, enter **0** to enable the conversation, and click **Set**.
 - Step 5** When prompted, click **OK**.
 - Step 6** Click **Exit**.
 - Step 7** Restart the Cisco Unity software for the registry change to take effect.
-

Securing Cisco Unity and the Cisco Unity Server

We strongly recommend that you secure Cisco Unity and the Cisco Unity server. Refer to the *Security Guide for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.



CHAPTER 9

Installing Optional Software

In this chapter, you do the following tasks in the order listed:

1. Install monitoring software, if applicable. See the “Installing Monitoring Software” section on page 9-1.
2. Install RSA SecurID, if applicable. See the “Installing RSA SecurID” section on page 9-1.
3. Install other optional software, if applicable. See the “Installing Other Optional Software” section on page 9-2.

When you are finished with this chapter, return to [Chapter 1, “Overview of Mandatory Tasks for Installing Cisco Unity”](#) to continue installing the Cisco Unity system.



Note

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Installing Monitoring Software

Follow the manufacturer instructions to install supported monitoring software.

Install only the monitoring agent on the Cisco Unity server. Do not install the full monitoring application.



Caution

If you install the full application—which is the default installation option for several of the monitoring applications we have tested—Cisco Unity will not function properly.

For information on supported software, refer to *Supported Hardware and Software, and Support Policies for Cisco Unity* at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Installing RSA SecurID

For supported versions of RSA SecurID, refer to *Supported Hardware and Software, and Support Policies for Cisco Unity* at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Follow the manufacturer instructions to install RSA SecurID.

The “[Overview of Mandatory Tasks for Installing Cisco Unity](#)” alerts you when to configure RSA SecurID later in the installation process.

Installing Other Optional Software

For information on supported software, refer to *Supported Hardware and Software, and Support Policies for Cisco Unity* at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Follow the manufacturer instructions to install other optional software.



CHAPTER 10

Setting Up Authentication for the Cisco Unity Administrator

In this chapter, you do the following tasks in the order listed:

1. Determine the authentication method that you want to use for the Cisco Unity Administrator. See the [“Determining the Authentication Method to Use for the Cisco Unity Administrator”](#) section on page 10-1.
2. Configure IIS so that the Cisco Unity Administrator and Status Monitor use the Anonymous authentication method, if applicable. See the [“Configuring IIS So That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication”](#) section on page 10-6.

When you are finished with this chapter, return to [Chapter 1, “Overview of Mandatory Tasks for Installing Cisco Unity”](#) to continue installing the Cisco Unity system.



Note

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Determining the Authentication Method to Use for the Cisco Unity Administrator

The Cisco Unity Administrator is the website used to do most administration tasks, including: determining system schedules, specifying settings for individual subscribers (or for a group of subscribers by using a subscriber template), and implementing a call management plan.

To access the Cisco Unity Administrator, Cisco Unity requires that the identity of the administrator is authenticated by a name and password. You can choose which IIS authentication method that you want to use for the Cisco Unity Administrator. (Note that the authentication method you choose also applies to the Cisco Unity Status Monitor.)



Note

Until a Cisco Unity subscriber account is created for the purpose of administering Cisco Unity, you must use the Windows credentials associated with the administration account that was selected when Cisco Unity was installed to log on to the Cisco Unity Administrator.

The following three subsections discuss the available authentication methods and how they work:

- [Authentication Methods Available for the Cisco Unity Administrator, page 10-2](#)

- [How Integrated Windows Authentication Works with the Cisco Unity Administrator, page 10-3](#)
- [How Anonymous Authentication Works with the Cisco Unity Administrator, page 10-4](#)

Authentication Methods Available for the Cisco Unity Administrator

By default, IIS is configured so that the Cisco Unity Administrator uses the Integrated Windows authentication method (formerly called NTLM or Windows NT Challenge/Response authentication) to authenticate the user name and password. If you prefer, you can configure IIS so that the Cisco Unity Administrator uses the Anonymous authentication method instead.

To determine which authentication method to use, first discuss it with the network administrator to confirm that the method you choose aligns with the existing authentication scheme in the organization and addresses security concerns for the site. In addition, consider the advantages and disadvantages of using each authentication method with the Cisco Unity Administrator, as shown in [Table 10-1](#) and [Table 10-2](#).

Refer to the Microsoft website for general information on the strengths and weaknesses of using either Integrated Windows or Anonymous authentication.

[Table 10-1](#) lists the advantages and disadvantages of using Integrated Windows authentication with the Cisco Unity Administrator.

Table 10-1 *Using Integrated Windows Authentication with the Cisco Unity Administrator*

Advantages	Disadvantages
<ul style="list-style-type: none"> • User credentials are not sent across the network. Instead, Internet Explorer and Windows use a challenge/response mechanism to authenticate the user. • By default, IIS is already set up so that the Cisco Unity Administrator uses the Integrated Windows authentication method. 	<ul style="list-style-type: none"> • Windows cannot validate the identity of a user when the user is logged on to an untrusted domain. To solve this problem, configure each subscriber browser to prompt for a user name and password so that subscribers can enter the applicable credentials for the domain that the Cisco Unity server is in. Alternatively, you can establish trusts across domains. • When subscribers log on to the Cisco Unity Administrator from another domain, they are prompted to re-enter their credentials each time that they want to use the phone as a recording and playback device for the Media Master.

Table 10-2 lists the advantages and disadvantages of using Anonymous authentication with the Cisco Unity Administrator.

Table 10-2 Using Anonymous Authentication with the Cisco Unity Administrator

Advantages	Disadvantages
<ul style="list-style-type: none"> • Subscribers can choose whether to enter their Domino or Windows credentials on the Cisco Unity Log On page. If subscribers use their Domino credentials, they do not need to have Windows domain accounts created for them. However, if subscribers have Windows domain accounts, they can use their Windows credentials to access the Cisco Unity Administrator if the Domino server goes down, for example. • When subscribers log on to the Cisco Unity Administrator from another domain, they can enter the applicable credentials on the Cisco Unity Log On page for the domain that the Cisco Unity server is in. Thus, you do not need to configure each subscriber browser to prompt for a user name and password, nor do you need to establish trusts across domains. • When subscribers log on to the Cisco Unity Administrator from another domain, they are not prompted to re-enter their credentials each time that they want to use the phone as a recording and playback device for the Media Master. 	<ul style="list-style-type: none"> • When a subscriber enters Domino credentials on the Cisco Unity Log On page, the credentials are sent across the network in clear text. To solve this problem, set up Cisco Unity to use SSL. • When a subscriber enters Windows domain account credentials on the Cisco Unity Log On page, the credentials are sent across the network in clear text. To solve this problem, set up Cisco Unity to use SSL. • By default, IIS is not set up so that the Cisco Unity Administrator uses the Anonymous authentication method. You must configure it.

How Integrated Windows Authentication Works with the Cisco Unity Administrator

When IIS is configured so that the Cisco Unity Administrator uses Integrated Windows authentication, Cisco Unity does not authenticate the subscriber. Instead, the identity of the user is verified by Windows.

1. A Cisco Unity subscriber starts Internet Explorer and attempts to browse to the Cisco Unity Administrator website.
2. Internet Explorer tries to get the home page for the Cisco Unity Administrator from IIS.
3. IIS indicates that it cannot authenticate the user.
4. When Internet Explorer is configured to prompt for a user name and password, it displays a dialog box and waits for the subscriber to enter the Windows domain account credentials. Once the subscriber enters the credentials, Internet Explorer tries to get the Cisco Unity Administrator web page again, but this time, it sends IIS an encrypted message regarding the Windows domain account based on the credentials that the subscriber entered in the dialog box.

When Internet Explorer is not configured to prompt for a user name and password, Internet Explorer tries to get the Cisco Unity Administrator web page again, but this time, it sends IIS an encrypted message regarding the Windows domain account based on the credentials that the subscriber entered to log on to Windows.

In both scenarios, the user password—or any representation of the password—is not sent across the network because authentication relies on Windows challenge/response.

5. If Windows can confirm the identity of the Windows domain user, then IIS sends the user and domain name to Cisco Unity, and the process continues with Step 6.

If Windows cannot validate the identity of the Windows domain user (as would be the case if the subscriber logged on to an untrusted domain), Internet Explorer prompts the subscriber for a user name and password. Once again, the credentials are not sent across the network; instead, Internet Explorer sends IIS an encrypted message regarding the Windows domain account based on the credentials that were entered in the dialog box. If Windows still cannot authenticate the user, Internet Explorer displays a message indicating that access to the website is denied because the domain account is unknown.

6. Cisco Unity checks to see that there is a subscriber account associated with the Windows domain account used to authenticate the subscriber and that the subscriber account has COS rights to access the Cisco Unity Administrator.
7. If a subscriber account exists and it has the proper COS rights, Cisco Unity presents the first page of the Cisco Unity Administrator website, which is displayed in the browser.

If the subscriber account does not exist or does not have the proper COS rights, Cisco Unity presents a web page that indicates that the subscriber does not have permission to view the Cisco Unity Administrator website.

How Anonymous Authentication Works with the Cisco Unity Administrator

When IIS is configured so that the Cisco Unity Administrator uses Anonymous authentication, Cisco Unity authenticates the credentials that subscribers enter on the Cisco Unity Log On page.

1. A Cisco Unity subscriber starts Internet Explorer and attempts to browse to the Cisco Unity Administrator website.
2. Internet Explorer tries to get the home page for the Cisco Unity Administrator from IIS.
3. IIS allows access to Cisco Unity based on the privileges for the IUSR_[computer name] account. (This is the anonymous account that IIS uses for Anonymous authentication by default.)
4. Cisco Unity presents the Cisco Unity Log On page, which is displayed in the browser.
5. By default, the Log On page prompts subscribers to enter the Domino credentials, as shown in [Table 10-3](#). However, subscribers can click the Log On Using Windows Authentication link provided on the Log On page to browse to another Log On page, as shown in [Table 10-4](#), on which they can enter their Windows domain account credentials.

Table 10-3 Cisco Unity Log On Page for Domino Credentials

Field Name	Description
Full Name	Subscribers must enter the full Lotus Notes user name that is associated with their Cisco Unity subscriber account. The full name consists of the user name, any organizational units that the Domino Person document resides in, and the IBM Domino certifier domain. (For example, subscribers can enter Terry Campbell/Sales/Cisco.)
Password	Subscribers must enter the Internet password for their Domino user account.

Table 10-4 Cisco Unity Log On Page for Windows Credentials

Field Name	Description
User Name	Subscribers must enter the alias for the Windows domain account that is associated with their Cisco Unity subscriber account. (For example, they can enter tcampbell or they can enter the full path, tcampbell@<domain name>.) If subscribers enter the full path for their alias, they do not need to complete the Domain field.
Password	Subscribers must enter the password for their Windows domain account.
Domain	Subscribers must enter the name of the domain in which their Windows domain account resides, unless they entered a full path for their alias in the User Name field. If that is the case, subscribers can leave the field blank.

6. Internet Explorer sends the credentials—in clear text—to Cisco Unity. (To solve this security problem, set up Cisco Unity to use SSL.)
7. When the subscriber has entered Domino credentials on the Log On page, Cisco Unity searches the Domino Address Book for a Person document associated with the user name that the subscriber entered on the Log On page. Once the user name is found, Cisco Unity retrieves the encrypted password from the Person document and compares it with the password that the subscriber entered on the Log On page. The process continues with Step 9.

(Note that by default, the connection between the Cisco Unity server and the Domino server is not encrypted. Refer to the Domino documentation for details on encrypting network data on a server port. It is also a good idea to discuss potential performance issues with the Domino administrator for the organization before enabling encryption on the Domino server.)
8. When the subscriber has entered Windows credentials on the Log On page, Cisco Unity requests authentication of the credentials from Windows. The process continues with Step 10.
9. If Cisco Unity can authenticate the Domino credentials, Cisco Unity confirms that there is a subscriber account associated with the Domino Person document used to authenticate the subscriber, and that the subscriber account has the proper COS rights. The process continues with Step 11.

If the credentials cannot be authenticated, Cisco Unity presents a web page that indicates that the subscriber does not have permission to view the Cisco Unity Administrator website.
10. If Cisco Unity can authenticate the Windows credentials, Cisco Unity then confirms that there is a subscriber account associated with the Windows domain account used to authenticate the subscriber and that the subscriber account has COS rights to access the Cisco Unity Administrator. The process continues with Step 11.

If the credentials cannot be authenticated, Cisco Unity presents a web page that indicates that the subscriber does not have permission to view the Cisco Unity Administrator website.
11. If the subscriber account exists and it has the proper COS rights, Cisco Unity presents the first page of the Cisco Unity Administrator website, which is displayed in the browser.

If the subscriber account does not exist or does not have the proper COS rights, Cisco Unity presents a web page, which indicates that the subscriber does not have permission to view the Cisco Unity Administrator website.

Configuring IIS So That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication



Note

If you decided that the Cisco Unity Administrator will use the Integrated Windows authentication method, skip this section.

This section contains two procedures. Do the applicable procedure, depending on whether the Cisco Unity server is running Windows Server 2003 or Windows 2000 Server.

To Configure IIS So That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication (Windows Server 2003)

-
- Step 1** On the Windows Start menu, click **Administrative Tools > Internet Information Services (IIS) Manager**.
- Step 2** In the left pane, right-click **Application Pools**, and click **Properties**.
- Step 3** In the Application Pools Properties dialog box, click the **Identity** tab.
- Step 4** In the Predefined list, click **Local System**.
- Step 5** Click **OK** to close the Application Pools Properties dialog box.
- Step 6** In the IIS Manager message box, click **Yes** to confirm that you want to run this application pool as Local System.
- Step 7** In the left pane of Internet Information Services (IIS) Manager, expand **Web Sites > Default Web Site**.
- Step 8** Right-click **SAWeb**, and click **Properties**.
- Step 9** In the SaWeb Properties dialog box, click the **Directory Security** tab.
- Step 10** In the Authentication and Access Control section, click **Edit**.
- Step 11** In the Authentication Methods dialog box, check the **Enable Anonymous Access** check box.
- Step 12** Uncheck the **Integrated Windows Authentication** check box.
- Step 13** Click **OK** to close the Authentication Methods dialog box.
- Step 14** Click **OK** to close the SaWeb Properties dialog box.
- Step 15** Repeat [Step 8](#) through [Step 14](#) for the following virtual directories:
- Status
 - StatusXml
 - Web
- Step 16** In the left pane, click **StatusXml**.
- Step 17** In the right pane, right-click **AvXml.dll**, and click **Properties**.
- Step 18** In the AvXml.dll Properties dialog box, click the **File Security** tab.
- Step 19** In the Authentication and Access Control section, click **Edit**.
- Step 20** In the Authentication Methods dialog box, check the **Enable Anonymous Access** check box.
- Step 21** Uncheck the **Integrated Windows Authentication** check box.
- Step 22** Click **OK** to close the Authentication Methods dialog box.

- Step 23** Click **OK** to close the AvXml.dll Properties dialog box.
- Step 24** Close Internet Information Services (IIS) Manager.
-

To Configure IIS So That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication (Windows 2000 Server)

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
- Step 2** In the Internet Information Services window, double-click **<System-name>** to expand it.
- Step 3** Under Default Web Site, right-click **Web**, and click **Properties**.
- Step 4** In the Properties dialog box, set the authentication method for the Web directory:
- Click the **Directory Security** tab.
 - Under Anonymous Access and Authentication Control, click **Edit**.
 - In the Authentication Methods dialog box, check the **Anonymous Access** check box.
 - Uncheck the **Integrated Windows Authentication** check box.
 - Click **OK** to close the Authentication Methods dialog box.
 - Click **OK** to close the Properties dialog box.
- Step 5** Under Default Web Site, right-click **SAWeb**, and click **Properties**.
- Step 6** Repeat [Step 4](#) to set the authentication method for the SAWeb directory.
- Step 7** Under Default Web Site, right-click **Status**, and click **Properties**.
- Step 8** Repeat [Step 4](#) to set the authentication method for the Status directory.
- Step 9** Under Default Web Site, click **AvXML**.
- Step 10** In the AvXML directory, right-click **AvXML.dll**, and click **Properties**.
- Step 11** Repeat [Step 4](#) to set the authentication method for AvXML.dll.
- Step 12** Close the Internet Information Services window.
-



APPENDIX **A**

Voice Cards and PIMG Units

This appendix contains the following sections:

- [Intel Dialogic D/41EPCI, D/41JCT-LS, and D/41JCT-Euro, page A-1](#)
- [Intel Dialogic D/120JCT-LS and D/120JCT-Euro, page A-4](#)
- [Intel Dialogic D/240PCI-T1, page A-8](#)
- [Intel NetStructure PBX-IP Media Gateway \(PIMG\), page A-11](#)

Intel Dialogic D/41EPCI, D/41JCT-LS, and D/41JCT-Euro

The D/41EPCI, D/41JCT-LS, and D/41JCT-Euro voice cards provide four independent voice-processing ports in a single PCI slot. The cards connect four phone-line interface circuits directly to analog loop-start lines by using RJ-11 connectors.

If you are installing cards that have H.100 connectors, you need an H.100 cable that has at least as many connectors as you have cards (you must connect all cards by using a single cable) but no more than five extra connectors.

Figure A-1 D/41EPCI Top and Side Views

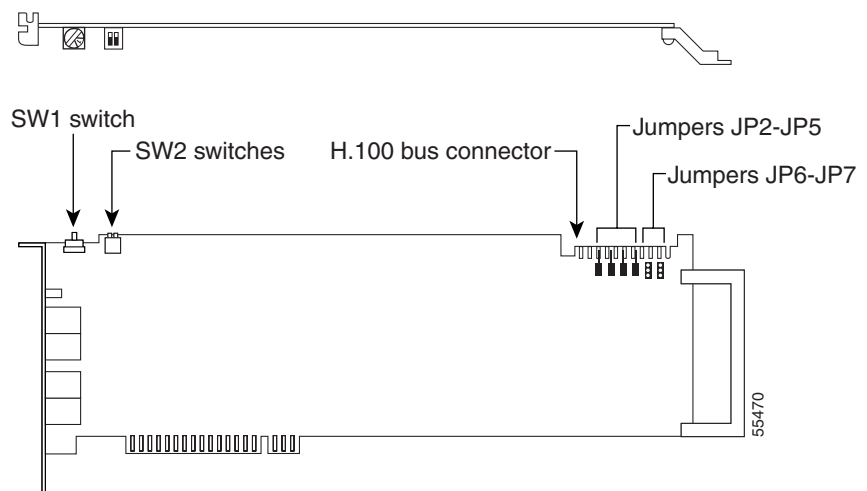


Figure A-2 D/41JCT-LS, and D/41JCT-Euro Top and Side Views

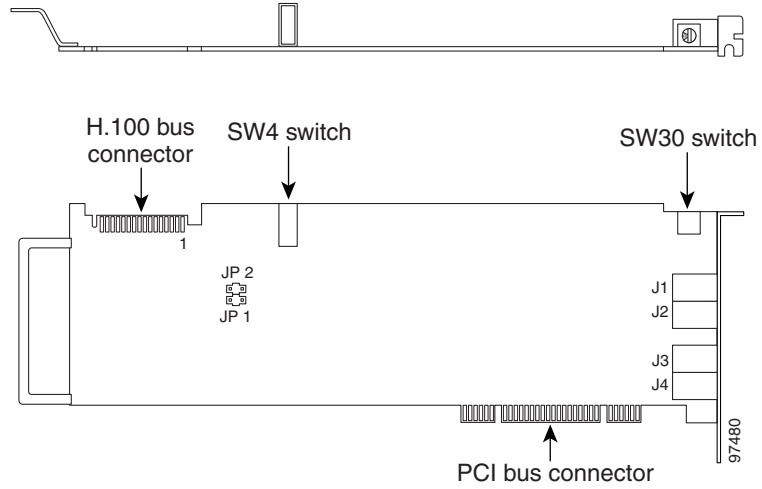
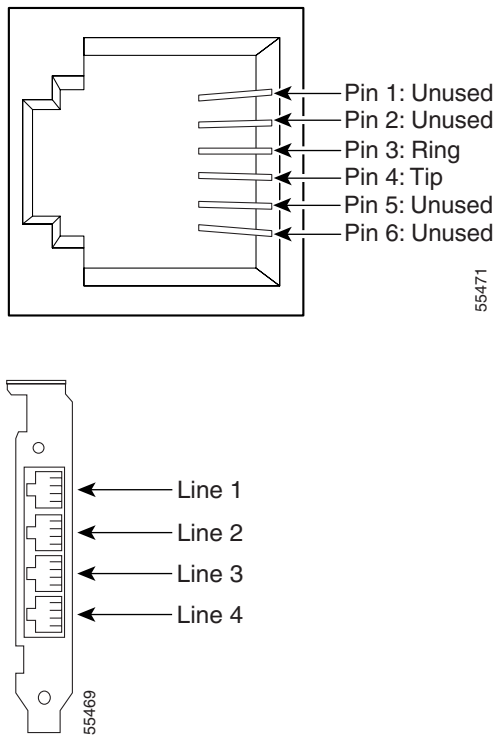


Figure A-3 D/41EPCI, D/41JCT-LS, and D/41JCT-Euro Connection Pinouts and Backplate

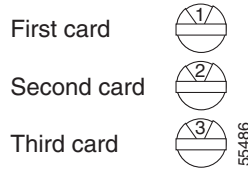


Hardware Settings

To Set the D/41EPCI Card Switches and Jumpers

- Step 1** Set the rotary switch (SW1) to a unique value for each card.

Each Intel Dialogic card in the Cisco Unity server or expansion chassis must have a unique value, starting with **1** and continuing in sequence on subsequent cards. For example, set the rotary switch on the first three voice cards as shown below. This is also the order in which you install the cards in the server or expansion chassis.



Step 2 Set SW2 switches to **Off** on each card.

Step 3 Settings for jumpers JP2 through JP5 depend on the number of D/41EPCI voice cards in the Cisco Unity server or expansion chassis:

One card	Set jumpers JP2 through JP5 to Off (Figure A-4) on the card.
Two cards	Set jumpers JP2 through JP5 to On (Figure A-5) on both cards.
Three or more cards	Set jumpers JP2 through JP5 to On (Figure A-5) on the first and last cards. Set jumpers JP2 through JP5 to Off (Figure A-4) on all other cards.

Figure A-4 D/41EPCI Jumpers JP2 Through JP 5: Off

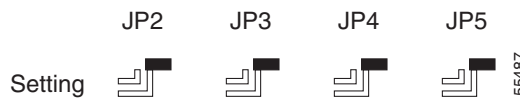
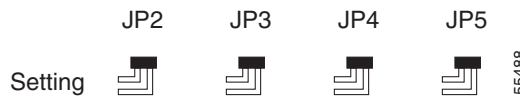
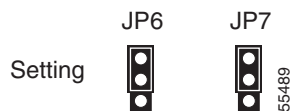


Figure A-5 D/41EPCI Jumpers JP2 Through JP 5: On



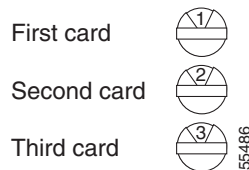
Step 4 On jumpers JP6 and JP7, install shunts on the top two pins (1 and 2).



To Set the D/41JCT-LS and D/41JCT-Euro Card Switches and Jumpers

Step 1 Set the rotary switch (SW30) to a unique value for each card.

Each Intel Dialogic card in the Cisco Unity server or expansion chassis must have a unique value, starting with **1** and continuing in sequence on subsequent cards. For example, set the rotary switch on the first three voice cards as shown below. This is also the order in which you install the cards in the Cisco Unity server or expansion chassis.



Step 2 Set the SW4 hook-state switch to **Off**.

Step 3 Settings for jumpers JP1 and JP2 are as follows:

Jumper JP1 is reserved. Do not install a shunt across the pins of JP1.

Set jumper JP2 according to the number of D/41JCT-LS or D/41JCT-EURO cards in the server or expansion chassis:

One card	Unterminated (the default configuration).
Two or more cards	Install the shunt on the JP2 jumper of a card to terminate the CT bus (H.100 signal) at that card. Terminate only the first and last cards on the CT bus cable.

Intel Dialogic D/120JCT-LS and D/120JCT-Euro

The D/120JCT-LS and D/120JCT-Euro voice cards each provide 12 channels of call-processing and loop-start interfaces in a single PCI slot. The D/120JCT-LS is used in North America, South America, and Japan, and the D/120JCT-Euro is used in Europe, Australia, and New Zealand. The cards connect 12 analog loop-start phone lines to 12 onboard call-processing resources by using RJ-14 connectors.

We recommend using the newer Revision 2 Universal (3.3Vdc or 5Vdc dual voltage) PCI versions of the Intel Dialogic D/120JCT-LS and the D/120JCT-Euro cards, rather than the older single-bus voltage (5Vdc) versions of the cards.

Note that older Revision 1 LS cards are still supported for use with Cisco Unity version 4.0(x), but they cannot be ordered for new Cisco Unity version 4.0(x) installations. In addition, the older LS cards can be used only when they are appropriate for the available slots in the Cisco Unity server or expansion chassis.

If you are installing cards that have H.100 connectors, you need an H.100 cable that has at least as many connectors as you have cards (you must connect all cards by using a single cable) but no more than five extra connectors.

You may need to attach or remove the slot retainer bracket that ships with the card, depending on the mechanical configuration of the Cisco Unity server or expansion chassis.

Figure A-6 *D/120JCT-LS and D/120JCT-Euro Rev 1 (Conventional PCI) Top and Side Views*

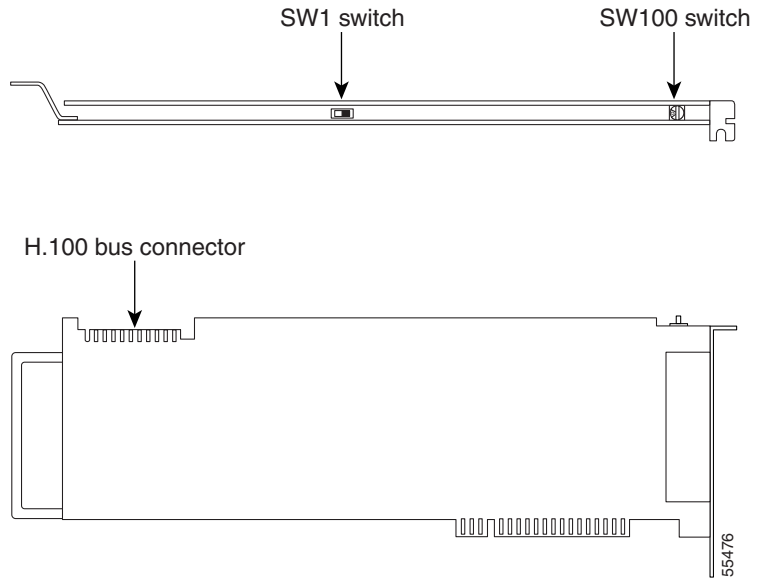


Figure A-7 *D/120JCT-LS and D/120JCT-Euro Rev 2 (uPCI) Top and Side Views*

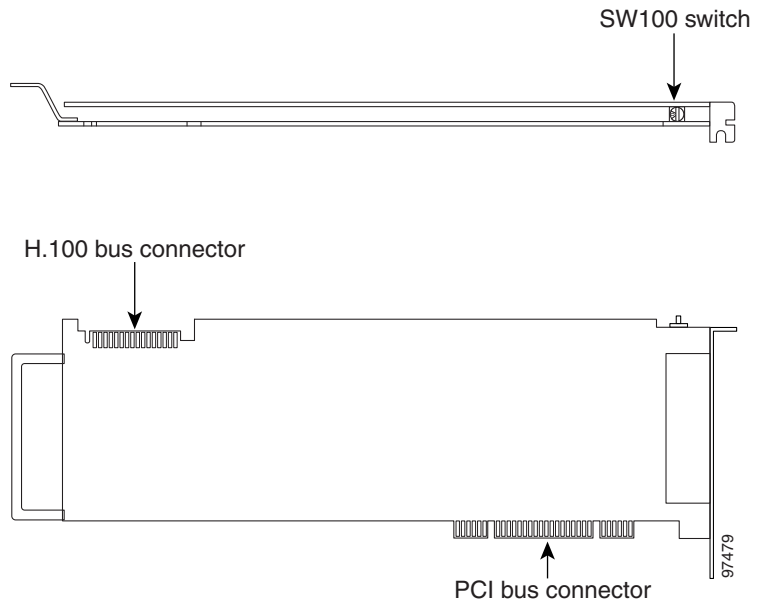
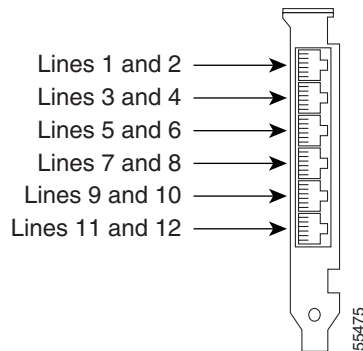
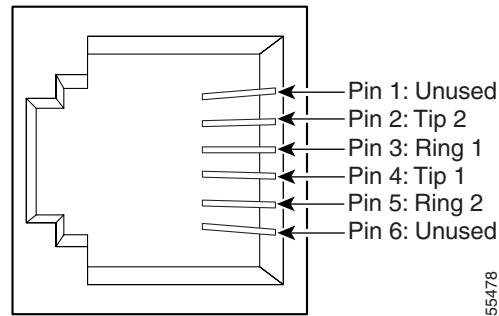


Figure A-8 D/120JCT-LS and D/120JCT-Euro Connection Pinouts and Backplate

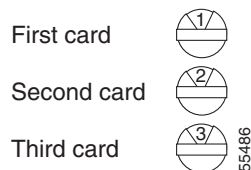


Hardware Settings

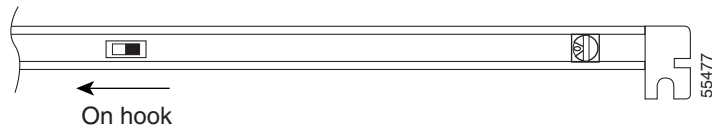
To Set the D/120JCT-LS and D/120JCT-Euro Card Switches

- Step 1** Set the rotary switch (SW100) to a unique value for each card.

Each Intel Dialogic card in the Cisco Unity server or expansion chassis must have a unique value, starting with **1** and continuing in sequence on subsequent cards. For example, set the rotary switch on the first three voice cards as shown below. This is also the order in which you install the cards in the server.



- Step 2** Set the SW1 switch to **On Hook** on each card.



Software Settings

Do the following procedure only if the Cisco Unity server contains D/120JCT-Euro voice cards. There are no software settings for D/120JCT-LS voice cards.

To Select the Country for D/120JCT-Euro Voice Cards

- Step 1** Exit the Cisco Unity software, if it is running. For more information, see [Appendix B, “Exiting and Starting the Cisco Unity Software and Server.”](#)
- Step 2** Click **Programs > Administrative Tools > Services**.
- Step 3** In the right pane of the Services dialog box, right-click **Telephony**, and click **Stop**.
- Step 4** If you are prompted to stop other services, click **Yes**.
- Step 5** On the Windows Start menu, click **Programs > Dialogic System Software > Dialogic Configuration Manager–DCM**.
- Step 6** When the message “DCM could not detect devices...” appears, click **OK**.
- Step 7** In the DCM toolbar, click the red button to stop the Dialogic service.
- Step 8** When the Dialogic service has stopped, click **Close**.
- Step 9** In the Dialogic Configuration Manager dialog box, in the list of installed cards, double-click a D/120JCT-Euro card.
- Step 10** In the Dialogic Configuration Manager Properties dialog box, click the **Country** tab.
- Step 11** In the Country list, click the applicable value:

Euro (CTR-21)	For all countries that require CE conformity, including Austria, Belgium, Denmark, Finland, France, Germany, Greece, Hong Kong, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, and the United Kingdom.
Australia	For Australia.
New Zealand	For New Zealand.

- Step 12** If you chose Australia or New Zealand in the Country list, then in the Frequency Resolution list, click **FREQRES_LOW**.
- Step 13** Click **OK**.
- Step 14** Repeat Steps 9 through 13 for each D/120JCT-Euro card installed in the system.

- Step 15** Close the DCM.
- Step 16** Restart the Cisco Unity server.
-

Intel Dialogic D/240PCI-T1

The Dialogic D/240PCI-T1 voice card provides one T1 span with 24 channels of voice processing in a single PCI slot. The card connects directly to a channel-service unit, digital-service unit, or to other phone-network terminating equipment by using an RJ-48C connector.

If you are installing cards that have H.100 connectors, you need an H.100 cable that has at least as many connectors as you have cards (you must connect all cards by using a single cable) but no more than five extra connectors.

Figure A-9 D/240PCI-T1 Top and Side Views

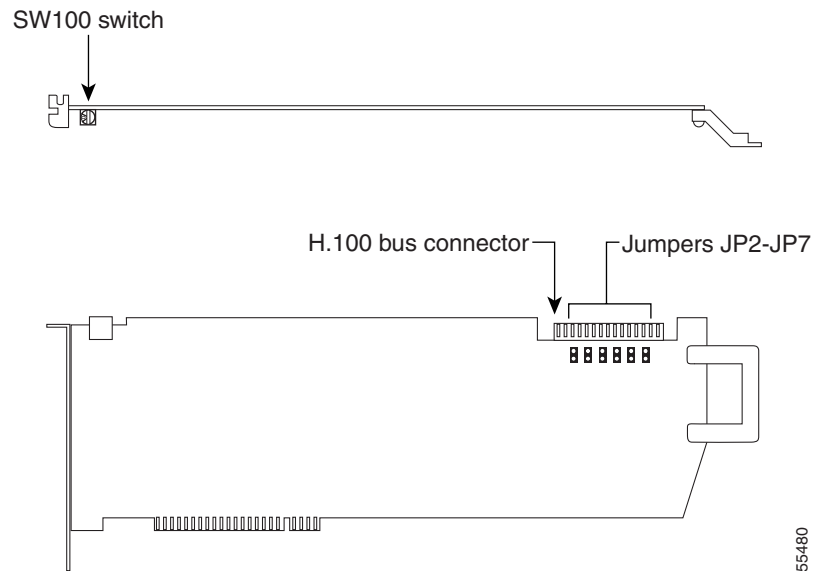
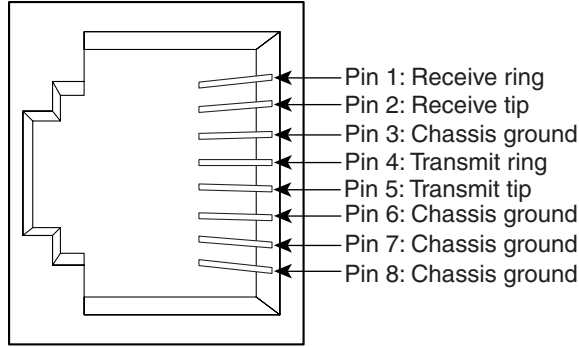
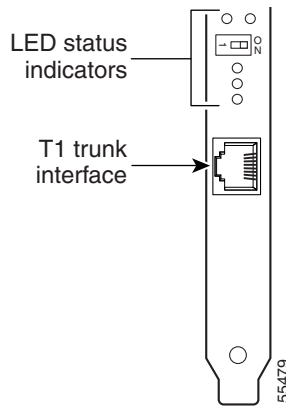


Figure A-10 D/240PCI-T1 Connection Pinouts and Backplate



55481



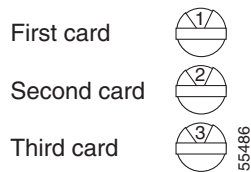
55479

Hardware Settings

To Set the D/240PCI-T1 Card Switches and Jumpers

Step 1 Set the rotary switch (SW100) to a unique value.

Each Intel Dialogic card in the Cisco Unity server or expansion chassis must have a unique value, starting with **1** and continuing in sequence on subsequent cards. For example, set the rotary switch on the first three voice cards as shown below. This is also the order in which you install the cards in the server.



55486

- Step 2** Settings for jumpers JP2 through JP5 depend on the number of D/240PCI-T1 voice cards in the Cisco Unity server:

One card	Set jumpers JP2 through JP5 to Off (Figure A-11) on the card.
Two cards	Set jumpers JP2 through JP5 to On (Figure A-12) on both cards.
Three or more cards	Set jumpers JP2 through JP5 to On (Figure A-12) on the first and last cards. Set jumpers JP2 through JP5 to Off (Figure A-11) on all other cards.

Figure A-11 D/240PCI-T1 Jumpers JP2 Through JP 5: Off

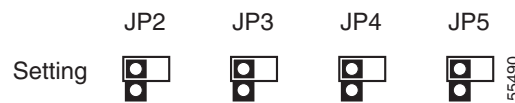
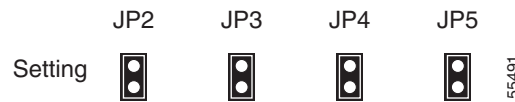
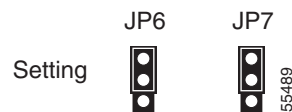


Figure A-12 D/240PCI-T1 Jumpers JP2 Through JP 5: On



- Step 3** On jumpers JP6 and JP7, install shunts on the top two pins (1 and 2).



Software Settings

For a D/240PCI-T1 voice card, set the protocol manually after the Cisco Unity Setup program is finished.

To Set the D/240PCI-T1 Protocol

- Step 1** On the Windows Start menu, click **Settings > Control Panel > Phone and Modem Options**.
- Step 2** In the Phone and Modem Options dialog box, click the **Advanced** tab.
- Step 3** Click **Dialogic Generation 2 Service Provider for NT**.
- Step 4** Click **Configure**.
- Step 5** In the Dialogic TSP Configuration dialog box, click **Advanced**.
- Step 6** In the Configuration Service dialog box, click the **Digital Protocols** tab.
- Step 7** In the Currently Assigned Protocols list, click **DtiB1 Undefined Protocol**.

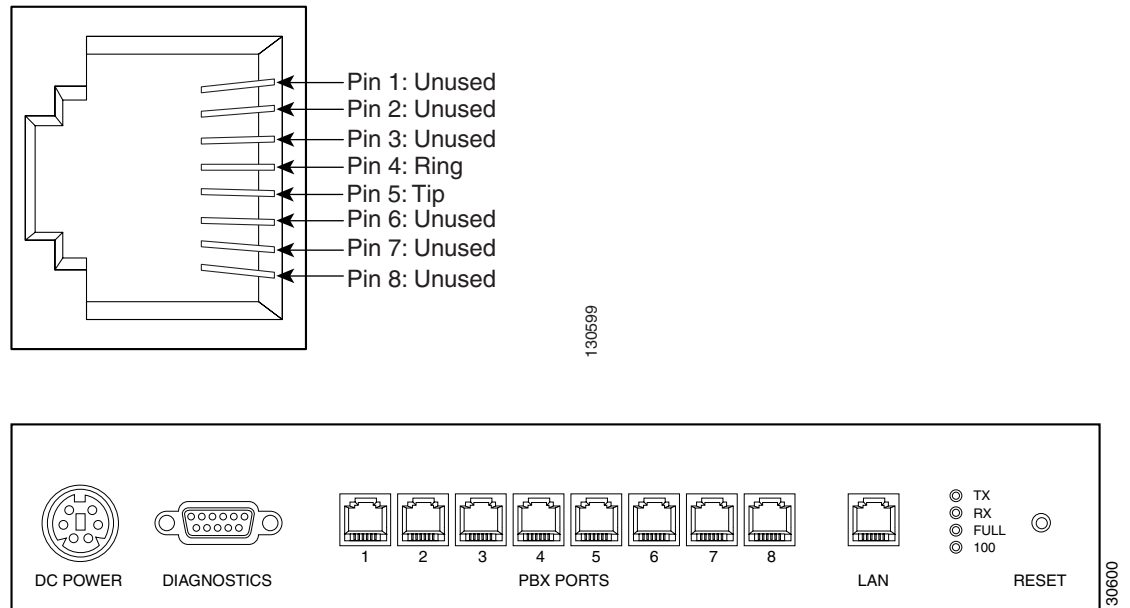
- Step 8** In the Available Protocols list, click **Us_ls_fxs_io**.
- Step 9** Click **Set Protocol**. DtiB1 Undefined Protocol changes to Us_ls_fxs_io.
- Step 10** If the Currently Assigned Protocols list contains more than one item (when the Cisco Unity server contains more than one D/240PCI-T1 card), repeat Steps 7 through 9 to change the remaining items from DtiB1 Undefined Protocol to Us_ls_fxs_io.
- Step 11** Click **OK** to close the Configuration Service dialog box.
- Step 12** Click **OK** to close the Dialogic TSP Configuration dialog box.
- Step 13** Click **Close** to close the Phone and Modem Options dialog box.
- Step 14** Close Control Panel.

Intel NetStructure PBX-IP Media Gateway (PIMG)

The Intel NetStructure PBX-IP Media Gateway (PIMG) units each connect to eight ports from a circuit-switched phone system (either analog or digital phone lines, depending on the model of the PIMG unit). The PIMG units communicate with the Cisco Unity server through the LAN by using Session Initiation Protocol (SIP).

The lines from the phone system attach to a PIMG unit with RJ-45 connectors, though it is possible to use RJ-11 connectors on these lines instead.

Figure A-13 PIMG Unit Connection Pinout and Port Connections



We recommend that the lines connect to the ports on the PIMG units in the same order as the ports on the phone system. For example, the first phone system port connects to the first port on the PIMG unit, the second phone system port connects to the second port on the PIMG unit, and so on.

Software Settings

Instructions for configuring PIMG units for integrating a phone system with Cisco Unity are found in the applicable Cisco Unity integration guide, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.



APPENDIX **B**

Exiting and Starting the Cisco Unity Software and Server

This appendix contains the following sections:

- [Exiting the Cisco Unity Software, page B-1](#)
- [Shutting Down or Restarting the Cisco Unity Server, page B-3](#)
- [Starting the Cisco Unity Software, page B-3](#)

Exiting the Cisco Unity Software

This section contains two procedures for exiting the Cisco Unity software: from the Cisco Unity server and from another computer.



Caution

Do not use `Kill av*.*` to exit the Cisco Unity software. `Kill av*.*` does not stop all Cisco Unity services. Do not stop AvCsMgr by using the Services window or the Component Services window as a method to exit the Cisco Unity software. Stopping the AvCsMgr does not stop all Cisco Unity services and may cause unexpected results.

To Exit the Cisco Unity Software from the Cisco Unity Server

- Step 1** If the system uses the automated attendant, route all calls to the operator.
 - Step 2** On the Cisco Unity server, log on to Windows by using either the Cisco Unity administration account or an appropriate Windows domain account.
 - Step 3** Right-click the **Cisco Unity** icon in the status area of the taskbar.
(If the Cisco Unity icon is not in the taskbar, browse to the CommServer directory, and double-click AvCsTrayStatus.exe.)
 - Step 4** Click **Stop Cisco Unity**.
 - Step 5** Click **OK** to confirm that you want to exit the Cisco Unity software. Cisco Unity stops running when all calls are finished, and an “X” appears in the Cisco Unity icon.
 - Step 6** Press **Ctrl-Alt-Delete**, then lock or log off of Windows to prevent access by unauthorized users.
-

To Exit the Cisco Unity Software from Another Computer

- Step 1** If the system uses the automated attendant, route all calls to the operator.
- Step 2** If the Cisco Unity Status Monitor does not use Integrated Windows authentication, skip to [Step 3](#).
When the Cisco Unity Status Monitor uses Integrated Windows authentication, do the following substeps to access the Status Monitor:
- a. Log on to Windows by using either the Cisco Unity administration account or an appropriate Windows domain account.
 - b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
 - c. If Internet Explorer prompts you for a user name and password, enter the user name, password, and domain for the administration account or the Windows domain account.
 - d. Skip to [Step 6](#).
- Step 3** When the Cisco Unity Status Monitor uses Anonymous authentication, do the following substeps to access the Status Monitor:
- a. Log on to Windows by using any domain account that has the right to log on locally.
 - b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
- Step 4** On the Cisco Unity Log On Page, do one of the following:
- Enter the full name and Internet password of a Domino account that is associated with an appropriate Cisco Unity subscriber account, and click **Log On**, then skip to [Step 6](#).
 - Click **Log On Using Windows Authentication**.
- Step 5** On the Cisco Unity Log On page, enter the user name, password, and domain for the Cisco Unity administration account or the Windows domain account, and click **Log On**.
- Step 6** In the Cisco Unity Status Monitor, under Shutting Down Cisco Unity, choose a method:
- Cisco Unity stops running after all calls are finished.
 - Cisco Unity interrupts calls in progress with a voice message, disconnects all calls, then stops running.
- Step 7** Click **Shut Down**.
-

Shutting Down or Restarting the Cisco Unity Server

If the Cisco Unity system has an expansion chassis or is set up for failover, note the following considerations before shutting down or restarting the Cisco Unity server:

Expansion chassis connected to the Cisco Unity server	When both the expansion chassis and the Cisco Unity server are turned off, turn on the expansion chassis before you turn on the server. Otherwise, the server may not detect the voice cards in the expansion chassis.
Cisco Unity failover	<ul style="list-style-type: none"> • When both servers are running and the active server is shut down, the inactive server becomes active. • When neither server is running, the first server started becomes the active server. • When the secondary server is active and configured for automatic failback, and the primary server is also running, the secondary server attempts failback on the failback schedule.

To Shut Down or Restart the Cisco Unity Server

-
- Step 1** Exit the Cisco Unity software, if it is running, by using one of the procedures in the [“Exiting the Cisco Unity Software”](#) section on page B-1.
- Step 2** On the Windows Start menu, click **Shut Down**.
- Step 3** Click **Shut Down** or **Restart**. During a restart, the Cisco Unity software starts automatically.
- When Cisco Unity starts successfully, three tones play and a check mark appears in the Cisco Unity icon in the status area of the taskbar.
- When Cisco Unity does not start successfully, two tones play and an “X” appears in the Cisco Unity icon in the status area of the taskbar.
-

Starting the Cisco Unity Software

This section contains two procedures for starting the Cisco Unity software: from the Cisco Unity server and from another computer.

Cisco Unity is a Windows service that is configured to start automatically when you turn on or restart the server. Do one of the procedures in this section only if you exited the Cisco Unity software and did not restart the server.

Domino must be running on the server that Cisco Unity connects with before you start the Cisco Unity software.

If Domino stops for any reason while Cisco Unity is running, Cisco Unity will continue to take messages.

To Start the Cisco Unity Software from the Cisco Unity Server

- Step 1** On the Cisco Unity server, log on to Windows by using either the Cisco Unity administration account or an appropriate Windows domain account.
- Step 2** Right-click the **Cisco Unity** icon in the status area of the taskbar.
(If the Cisco Unity icon is not in the taskbar, browse to the CommServer directory, and double-click **AvCsTrayStatus.exe**.)
- Step 3** Click **Start Cisco Unity**.
When Cisco Unity starts successfully, three tones play and a check mark appears in the Cisco Unity icon.
When Cisco Unity does not start successfully, two tones play and an “X” appears in the Cisco Unity icon.
- Step 4** Press **Ctrl-Alt-Delete**, then lock or log off of Windows to prevent access by unauthorized users.
- Step 5** If the system uses the automated attendant and you routed calls to the operator before you exited the Cisco Unity software, reroute calls to Cisco Unity.
-

To Start the Cisco Unity Software from Another Computer

- Step 1** If the Cisco Unity Status Monitor does not use Integrated Windows authentication, skip to [Step 2](#).
When the Cisco Unity Status Monitor uses Integrated Windows authentication, do the following substeps to access the Status Monitor:
- a. Log on to Windows by using either the Cisco Unity administration account or an appropriate Windows domain account.
 - b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
 - c. If Internet Explorer prompts you for a user name and password, enter the user name, password, and domain for the Cisco Unity administration account or the Windows domain account.
 - d. Skip to [Step 5](#).
- Step 2** When the Cisco Unity Status Monitor uses Anonymous authentication, do the following substeps to access the Status Monitor:
- a. Log on to Windows by using any domain account that has the right to log on locally.
 - b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
- Step 3** On the Cisco Unity Log On Page, do one of the following:
- Enter the full name and Internet password of a Domino account that is associated with an appropriate Cisco Unity subscriber account, and click **Log On**, then skip to [Step 5](#).
 - Click **Log On Using Windows Authentication**.
- Step 4** On the Cisco Unity Log On page, enter the user name, password, and domain for the Cisco Unity administration account or the Windows domain account, and click **Log On**.
- Step 5** In the Cisco Unity Status Monitor, click the **System Status** icon (the first icon), at the top of the page.
- Step 6** Click **Start**.

- Step 7** If the system uses the automated attendant and you routed calls to the operator before you exited the Cisco Unity software, reroute calls to Cisco Unity.
-



APPENDIX **C**

Installing and Configuring a Voice-Recognition Server

Use the following task list to install and configure voice-recognition software on a separate voice-recognition server. The tasks reference detailed instructions in the Cisco Unity installation guide as noted. Follow the documentation for a successful installation.

This appendix assumes that the Cisco Unity license includes voice recognition and that you are installing and configuring a voice-recognition server for a new Cisco Unity system. If you are adding a voice-recognition server to an existing Cisco Unity system, see the “Adding Voice Recognition” section in the “Adding Features to the Cisco Unity 5.x System” chapter in the applicable *Reconfiguration and Upgrade Guide for Cisco Unity* at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

1. Place the voice-recognition server in a dry, cool area that is free of dust and that is near a network connection.
2. Attach any supported peripheral devices to the server. Follow the manufacturer installation and test instructions.
3. If you are installing Windows Server 2003 using a retail Windows disk, configure the RAID arrays. See the “[Configuring the RAID Arrays \(Selected Installations\)](#)” section on page 4-3.
4. Install and configure Windows Server 2003 using the applicable procedure:
 - *If you bought the Cisco Unity server from Cisco:* See “[Installing Windows Server 2003 by Using the Cisco Unity Platform Configuration Discs](#)” section on page 4-4.
 - *If you bought the Cisco Unity server from another vendor:* See “[Installing Windows Server 2003 by Using a Retail Windows Server 2003 Disc](#)” section on page 4-8.



Caution Cisco Unity voice-recognition software cannot be installed on a server running Windows 2000 Server.

5. *If you installed Windows Server 2003 using a retail Windows disc:* Create the partitions according to the storage configuration requirements for the platform. See the “[Creating the Partition](#)” section on page C-2.
6. Install the required Windows service pack and updates and, optionally, Cisco Security Agent for Cisco Unity. See the “[Installing the Required Windows Server 2003 Service Pack and Updates, and Cisco Security Agent for Cisco Unity](#)” section on page C-3.
7. *If the Cisco Unity server contains a dual NIC:* Configure the dual NIC or verify the configuration. See the “[Configuring a Dual NIC in the Cisco Unity Server](#)” section on page 5-2.

8. Change folder settings in Windows Explorer so that all files and folders are visible during troubleshooting. See the [“Changing Folder Settings in Windows Explorer”](#) section on page 5-10.
9. *Optional:* Install antivirus software. See the [“Installing Antivirus Software \(Optional\)”](#) section on page 5-12.
10. Attach the network cable(s) to the voice-recognition server.
If the server contains a dual NIC, ensure that you connect the cable to the primary NIC, if you configured the dual NIC for AFT or NFT, or to the NIC that is enabled.
11. Configure TCP/IP properties. See the [“Configuring TCP/IP Properties”](#) section on page 5-12.
12. Confirm that the server has a valid IP address and is connected to the network. See the [“Verifying the IP Address and the Network Connection”](#) section on page 5-13.
13. *If antivirus software or Cisco Security Agent for Cisco Unity is installed on the server:* Disable antivirus and Cisco Security Agent for Cisco Unity services. See the [“Disabling Antivirus and Cisco Security Agent Services”](#) section on page 5-14.
14. *Optional:* Add the voice-recognition server as a member server in the same domain as the Cisco Unity server. (The server can also be a workgroup server.) See the [“Adding the Voice-Recognition Server to a Domain \(Optional\)”](#) section on page C-4.
15. Install Cisco Unity voice-recognition software on the voice-recognition server and on the Cisco Unity server. See the [“Installing Cisco Unity Voice-Recognition Software”](#) section on page C-5.
16. Configure the voice recognition software. See the [“Configuring Voice-Recognition Software”](#) section on page C-5.
17. *If antivirus software or Cisco Security Agent for Cisco Unity is installed on the server:* Exclude selected directories from virus scanning. See the [“Excluding Selected Directories from Virus Scanning”](#) section on page C-6.
18. Install the latest Windows Server 2003 service pack qualified for use with the Cisco Unity voice-recognition server, if any. In addition, run the latest Cisco Unity Server Updates wizard to install the latest updates recommended for use with the Cisco Unity voice-recognition server and, optionally, Cisco Security Agent for Cisco Unity. See the [“Installing the Latest Windows Server 2003 Service Pack and Updates”](#) section on page C-7.
19. *If antivirus software or Cisco Security Agent for Cisco Unity is installed on the server:* Re-enable antivirus and Cisco Security Agent for Cisco Unity services. See the [“Re-enabling Virus-Scanning and Cisco Security Agent Services”](#) section on page 8-22.
20. Install optional software on the voice-recognition server. See the [“Installing Optional Software”](#) chapter.

Creating the Partition



Note

If the Cisco Unity server was purchased from Cisco, skip this section. When you installed Windows using the Cisco Unity Platform Configuration discs shipped with the server, the partitions were created automatically.

The servers qualified for use as Cisco Unity voice-recognition servers have either one hard disk or one RAID array. A C: partition is created automatically when you install Windows. Do this procedure to create another partition in the remaining space on the hard disk or RAID array.

To Create the Partition

-
- Step 1** Log on to Windows as a member of the Administrators group.
 - Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Computer Management**.
 - Step 3** In the console tree under Storage, click **Disk Management**.
 - Step 4** Right-click the unallocated region after the C: partition, and click **New Partition**.
 - Step 5** On the New Partition Wizard, click **Next**.
 - Step 6** Click **Extended Partition**, and click **Next**. (Do not click Primary Partition.)
 - Step 7** Specify to use the remaining disk space, and click **Next**.
 - Step 8** Verify the settings, and click **Finish**.
 - Step 9** In the Disk Management utility, right-click the new partition, and click **New Logical Drive**.
 - Step 10** On the Create Partition Wizard welcome screen, click **Next**.
 - Step 11** Click **Logical Drive**, and click **Next**.
 - Step 12** Specify to use the maximum disk space, and click **Next**.
 - Step 13** Assign a drive letter, and click **Next**.
 - Step 14** Specify the NTFS file system format, and click **Next**.
 - Step 15** Verify the settings, and click **Finish**.
-

Installing the Required Windows Server 2003 Service Pack and Updates, and Cisco Security Agent for Cisco Unity

Revised May 1, 2008



Caution

Do not install the latest Windows Server 2003 service pack that is recommended for use with the Cisco Unity voice recognition yet. If a service pack was qualified for use with the current version of Cisco Unity voice recognition after the current version was released, it was not tested with Cisco Unity voice-recognition Setup and may cause Setup to fail.

You install the required Windows Server 2003 service pack from the applicable Cisco Unity Service Pack CD. The contents of the service pack CDs is listed in the *Release Notes for Cisco Unity* for your version of Cisco Unity. *Release Notes for Cisco Unity* are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

You run the Cisco Unity Server Updates wizard that you downloaded in the “[Downloading Software for the Installation](#)” section on page 2-2 to install the Microsoft updates that apply to Cisco Unity voice recognition and, optionally, to install Cisco Security Agent for Cisco Unity.

To Install the Required Windows Server 2003 Service Pack on the Cisco Unity Voice-Recognition Server

-
- Step 1** On the applicable Cisco Unity Service Packs CD, browse to the directory `Windows_2003_SP<x>\Setup\I386`, and double-click **Update.exe**.

■ Adding the Voice-Recognition Server to a Domain (Optional)

- Step 2** Follow the on-screen prompts to complete the installation.
- Step 3** Restart the server.

To Install Microsoft Updates and, Optionally, Cisco Security Agent for Cisco Unity

- Step 1** Insert in the drive the disc that you burned with the latest version of the Cisco Unity Server Updates Wizard.
- Step 2** Run **ServerUpdatesWizard.exe**.
- Step 3** Follow the on-screen prompts to complete the installation of Microsoft updates and, optionally, Cisco Security Agent for Cisco Unity.



Note

If you are accessing the server by using Remote Desktop or a VNC client, and you are installing Cisco Security Agent for Cisco Unity, the Remote Desktop or VNC session will be disconnected when Cisco Security Agent for Cisco Unity restarts the network interface. If the session does not reconnect automatically, reconnect manually to finish the Server Updates wizard.

- Step 4** Restart the Cisco Unity server.
-

Adding the Voice-Recognition Server to a Domain (Optional)

The voice-recognition server can be a workgroup server or a member server in the same domain as the Cisco Unity server. If you want make the server a member server, do the following procedure.

To Add the Voice-Recognition Server to the Same Domain as the Cisco Unity Server

- Step 1** Log on to the voice-recognition server by using an account that is a member of the local Administrators group.
- Step 2** On the Windows Start menu, click **Settings > Control Panel > System**.
- Step 3** Click the **Network Identification** tab.
- Step 4** Click **Properties**.
- Step 5** In the Identification Changes dialog box, click **Domain**, and enter the name of the domain of which the Cisco Unity server is a member.
- Step 6** Click **OK**.
- Step 7** In the Domain Username and Password dialog box, enter the name and password of an account that has permission to add computers to the domain.
- Step 8** Click **OK** three times.
- Step 9** Click **Yes** to restart the server.
-

Installing Cisco Unity Voice-Recognition Software

You install Cisco Unity voice-recognition software on the voice-recognition server and on the Cisco Unity server. Do the following two procedures in the specified order.

To Install Cisco Unity Voice-Recognition Software on the Voice-Recognition Server

- Step 1** Log on to the voice-recognition server by using an account that is a member of the local Administrators group.
 - Step 2** Insert Cisco Unity DVD_1 in the DVD drive.
 - Step 3** Browse to the UnityVoiceRecognitionSetup directory, and run **Setup.exe**.
 - Step 4** Follow the on-screen prompts until you are prompted to choose the location for voice-recognition files.
 - Step 5** Choose a location other than the system drive (drive C:) to install Cisco Unity voice-recognition software.
 - Step 6** Click **Next**.
 - Step 7** Accept the default location for the Cisco Unity voice-recognition service.
 - Step 8** Follow the on-screen prompts to complete the installation.
-

To Install Cisco Unity Voice-Recognition Software on the Cisco Unity Server

- Step 1** Log on to the Cisco Unity server by using an account that is a member of the local Administrators group.
 - Step 2** Insert Cisco Unity DVD 1 in the DVD drive.
 - Step 3** Browse to the UnityVoiceRecognitionSetup directory, and run **Setup.exe**.
 - Step 4** Follow the on-screen prompts to complete the installation.
-

Configuring Voice-Recognition Software

**Caution**

We recommend that you do the following procedure after hours. The manual update in [Step 7](#) is a processor- and memory-intensive process that will affect Cisco Unity performance.

To Configure the Voice-Recognition Server in Cisco Unity Administrator

- Step 1** On the Cisco Unity server, log on to Windows by using an account that is a member of the local Administrators group.
- Step 2** In the Cisco Unity Administrator, go to the **Configuration > Voice Recognition > Settings** page.
- Step 3** On the Voice Recognition Settings page, in the IP Address field, enter the IP address of the voice-recognition server. Note the following:

- Do not choose an address accessible from the Internet. Doing so can expose the voice-recognition server to unwanted intrusion from the Internet, even when the server is hardened.
- Do not choose an IP address that separates the voice-recognition server from the Cisco Unity by a firewall.

Step 4 Do not change the value of the **Socket Port** field.

Step 5 Change the value of **Limit Searches to the** as appropriate. For a detailed explanation of the available options, see the online Help.

Step 6 Click **Save**.

Step 7 Click **Start Manual Update**.

Cisco Unity will take up to 15 minutes to transfer licensing information and other data to the voice-recognition server. Until this process is complete, voice recognition will not function.

Step 8 Close Cisco Unity Administrator.

Excluding Selected Directories from Virus Scanning



Note

If antivirus software is not installed on the voice-recognition server, skip this section.

You exclude selected directories from virus scanning so that voice recognition will function properly.

To Exclude Selected Directories on the Voice-Recognition Server from Virus Scanning

Step 1 On the voice-recognition server, log on to Windows by using an account that is a member of the local Administrators group.

Step 2 Start the administration interface for the antivirus software.

Step 3 Exclude the following two directories from virus scanning:

- Nuance
- NuanceLogs



Caution

Do not configure antivirus software to block WAV attachments, or voice messages will be stripped of their recordings. In addition, do not configure antivirus software to scan WAV files, .log files, or .tmp files. Finally, do not configure antivirus software to block TCP or UDP port traffic, or h voice-recognition software may not function properly.

Refer to the antivirus software Help for instructions on excluding directories from scanning.

Installing the Latest Windows Server 2003 Service Pack and Updates

You install the latest Windows Server 2003 service pack that has been qualified for use with Cisco Unity voice recognition, as well as the corresponding updates, to enhance the security of the voice-recognition server. Do the following procedures.

To Install the Latest Windows Server 2003 Service Pack, If Any

Follow the instructions that you printed or downloaded when you downloaded the service pack.

To Install the Latest Microsoft Updates for Windows Server 2003

- Step 1** Insert in the drive the disc that you burned with the latest version of the Cisco Unity Server Updates Wizard.
- Step 2** Run **ServerUpdatesWizard.exe**.
- Step 3** Follow the on-screen prompts to complete the installation of Microsoft updates and, optionally, Cisco Security Agent for Cisco Unity.

**Note**

If you are accessing the server by using Remote Desktop or a VNC client, and you are installing Cisco Security Agent for Cisco Unity, the Remote Desktop or VNC session will be disconnected when Cisco Security Agent for Cisco Unity restarts the network interface. If the session does not reconnect automatically, reconnect manually to finish the Server Updates wizard.

- Step 4** Restart the Cisco Unity voice-recognition server.
-



INDEX

Numerics

3GB switch, adding to boot.ini for more than 96 ports [4-12](#)

A

accounts

- administration [7-2](#)
- creating for the Cisco Unity installation [7-2](#)
- directory and message store services [7-2](#)
- granting permissions for [7-4](#)
- installation [7-2](#)
- local services [7-2](#)
- required for the Cisco Unity installation [7-1](#)

Active Directory

- installing on Cisco Unity server [5-15](#)

adding

- administration account to an admins group [7-3](#)
- Cisco Unity server to existing domain [5-15](#)

administration account

- adding to an admins group [7-3](#)
- creating [7-2](#)
- description [7-2](#)

Anonymous authentication

- advantages and disadvantages of [10-2](#)
- how it works with Cisco Unity Administrator [10-4](#)
- using with Cisco Unity Administrator [10-2](#)

assigning IP address [5-12](#)

attaching peripheral devices to Cisco Unity server [3-4](#)

authentication, methods available for Cisco Unity Administrator [10-2](#)

B

boot.ini, adding switches for more than 96 ports [4-12](#)

browser, installing with Cisco Unity System Preparation Assistant [5-6](#)

C

challenge/response authentication [10-2](#)

changing folder settings in Windows Explorer [5-10](#)

Cisco Security Agent for Cisco Unity

- disabling service [5-14](#)
- downloading latest [2-3](#)
- re-enabling service [8-22](#)

Cisco Unity

- exiting software [B-1](#)
- restarting server [B-3](#)
- shutting down server [B-3](#)
- starting software [B-3](#)

Cisco Unity Administrator

- authentication methods available [10-2](#)
- description [10-1](#)
- setting up to use SSL [8-15](#)

Cisco Unity Installation and Configuration Assistant

- configuring Cisco Unity for message store [8-7](#)
- configuring services [8-7](#)
- description [8-3](#)
- installing Cisco Unity software [8-3](#)
- installing license files [8-6](#)
- integrating phone system with Cisco Unity [8-8](#)
- setting default passwords [8-8](#)
- setting up the Cisco PCA to use SSL [8-9](#)

Cisco Unity Install License File wizard, running [8-6](#)

Cisco Unity Message Store Configuration wizard, running [8-7](#)

Cisco Unity Permissions wizard, running [7-4](#)

Cisco Unity server

adding to existing domain [5-15](#)

attaching peripheral devices to [3-4](#)

connecting phone system to [3-4](#)

installing Active Directory [5-15](#)

physical location of [3-4](#)

securing [8-23](#)

Cisco Unity Services Configuration wizard, running [8-7](#)

Cisco Unity software

downloading for installation [2-2](#)

installing [8-3](#)

registering [5-4](#)

Cisco Unity System Preparation Assistant [5-6](#)

Cisco Unity Telephony Integration Manager, running [8-8](#)

configuring

Cisco Unity for message store [8-7](#)

Cisco Unity services [8-7](#)

Cisco Unity software [8-3](#)

dual NIC in Cisco Unity server [5-2](#)

IIS so Cisco Unity Administrator and Status Monitor use Anonymous authentication [10-6](#)

Lotus Notes to use Cisco Unity account [6-4](#)

RAID arrays [4-3](#)

TCP/IP properties [5-12](#)

connecting

peripheral devices to Cisco Unity server [3-4](#)

phone system [3-4](#)

conventions, documentation [2-vii](#)

creating

accounts for the Cisco Unity installation [7-2](#)

partitions [4-11](#)

D

D/120JCT-Euro [A-4](#)

D/120JCT-LS [A-4](#)

D/240PCI-T1 [A-8](#)

D/41EPCI [A-1](#)

D/41JCT-Euro [A-1](#)

D/41JCT-LS [A-1](#)

databases, SQL Server 2000 or MSDE 2000, moving [8-19](#)

demonstration system, default license file for [5-6](#)

Dialogic. *See* voice cards

directory and message store services account

creating [7-2](#)

description [7-2](#)

granting permissions with Cisco Unity Permissions wizard [7-4](#)

disabling

Cisco Security Agent service [5-14](#)

Found New Hardware wizard for voice cards [5-11](#)

virus-scanning services [5-14](#)

documentation

audience and use [2-vii](#)

conventions [2-vii](#)

required for the Cisco Unity installation [2-1](#)

domain

accounts required for the Cisco Unity installation [7-1](#)

adding Cisco Unity server to existing [5-15](#)

Domino

preparing server(s) for Cisco Unity [6-1](#)

running Cisco Unity Permissions wizard for [7-4](#)

downloading firmware for PBXLink boxes or PIMG units [2-3](#)

downloading software for installation [2-2](#)

drive locations for files, determining [2-4](#)

drivers-missing error message [3-1](#)

dual NIC, configuring [5-2](#)

E

enabling

Unity Messaging Repository conversation [8-22](#)

error message, unknown PCI device [3-1](#)

Example Administrator account, securing against toll fraud [8-18](#)
 excluding from virus scanning directory in which Cisco Unity is installed [8-14](#)
 exiting Cisco Unity software [B-1](#)

F

files, drive locations for [2-4](#)
 firmware, downloading for PBXLink boxes or PIMG units [2-3](#)
 folder settings, changing in Windows Explorer [5-10](#)
 Found New Hardware wizard, disabling for voice cards [5-11](#)

G

granting permissions with Cisco Unity Permissions wizard [7-4](#)

H

hardening Cisco Unity server [8-23](#)

I

IIS, configuring so Cisco Unity Administrator and Status Monitor use Anonymous authentication [10-6](#)

installation

- accounts required for [7-1](#)
- overview of mandatory tasks [1-1](#)
- required documentation for [2-1](#)

installation account

- creating [7-2](#)
- description [7-2](#)

installing

- Active Directory on Cisco Unity server [5-15](#)
- administration software for MSDE 2000 [5-9](#)
- browser with Cisco Unity System Preparation Assistant [5-6](#)

Cisco Unity software [8-3](#)
 license files [8-6](#)
 Lotus Notes on Cisco Unity server [6-4](#)
 Microsoft Certificate Services component [8-3](#)
 monitoring software [9-1](#)
 MSDE 2000 with Cisco Unity System Preparation Assistant [5-6](#)
 NIC-configuration utility [5-3](#)
 optional software [9-2](#)
 RSA SecurID [9-1](#)
 service packs and updates with Cisco Unity System Preparation Assistant [5-6](#)
 SQL Server 2000 with Cisco Unity System Preparation Assistant [5-6](#)
 updates for Windows, Internet Explorer, and SQL Server 2000 or MSDE 2000 [5-10](#)
 virus-scanning software [5-12](#)
 voice cards [3-1](#)
 Windows 2000 Server using the PCD [4-4, 4-6](#)
 Windows components with Cisco Unity System Preparation Assistant [5-6](#)
 Windows Server 2003 using the PCD [4-4](#)

Integrated Windows authentication

- advantages and disadvantages of [10-2](#)
- how it works with Cisco Unity Administrator [10-3](#)
- using with Cisco Unity Administrator [10-2](#)

integrating phone system with Cisco Unity [8-8](#)

Intel Dialogic. *See* voice cards

Intel NetStructure PBX-IP Media Gateway (PIMG) [A-11](#)

IP address

- assigning [5-12](#)
- verifying [5-13](#)

J

jumpers and switches

- D/240PCI-T1 [A-9](#)
- D/41EPCI [A-2](#)
- D/41JCT-LS and D/41JCT-Euro [A-4](#)

L

license files

- default for Cisco Unity demonstration system [5-6](#)
- getting a replacement copy [5-5](#)
- installing [8-6](#)
- obtaining [5-4](#)

local services account [7-2](#)

logs

- SQL Server 2000 or MSDE 2000, moving [8-19](#)

Lotus Notes

- configuring to use Cisco Unity account [6-4](#)
- installing on Cisco Unity server [6-4](#)

MMAC address of Cisco Unity server [5-4](#)message store, configuring Cisco Unity for [8-7](#)Microsoft Certificate Services component, installing [8-3](#)Microsoft updates, installing [5-10](#)missing-drivers error message [3-1](#)monitoring software, installing [9-1](#)

moving

- SQL Server 2000 or MSDE 2000 databases and transaction logs [8-19](#)

MSDE 2000

- installing administration software for [5-9](#)
- installing with Cisco Unity System Preparation Assistant [5-6](#)
- moving databases and transaction logs [8-19](#)
- setting sa password [5-9](#)

N

network

- securing Cisco Unity server [8-23](#)
- verifying connection [5-13](#)

network interface card. *See* NIC [5-2](#)

NIC

configuration utility, installing [5-3](#)

configuring dual [5-2](#)

non-universal PCI cards, slot placement [3-1](#)

NTLM authentication [10-2](#)

O

obtaining license files [5-4](#)

optional software, installing [9-2](#)

P

PAK, location of [5-4](#)

partitions, creating [4-11](#)

Password Hardening wizard, running [8-8](#)

passwords

changing for the Example Administrator account [8-18](#)

sa for MSDE 2000 [5-9](#)

setting default [8-8](#)

PBX-IP Media Gateway (PIMG) [A-11](#)

PBXLink boxes, downloading firmware [2-3](#)

peripheral devices, attaching [3-4](#)

permissions

granting with Cisco Unity Permissions wizard [7-4](#)

Permissions wizard, running [7-4](#)

phone system

integrating with Cisco Unity and testing integration [8-8](#)

making connections from [3-4](#)

PIMG units [A-11](#)

connecting phone system to [3-4](#)

PIMG units, downloading firmware [2-3](#)

preparing Domino server(s) for Cisco Unity [6-1](#)

product authorization key, location of [5-4](#)

R

RAID arrays

- configuring [4-3](#)
- re-enabling
 - Cisco Security Agent service [8-22](#)
 - virus-scanning services [8-22](#)
- registering Cisco Unity software [5-4](#)
- restarting
 - Cisco Unity server [B-3](#)
- RSA SecurID, installing [9-1](#)

S

- sa password, setting for MSDE 2000 [5-9](#)
- securing
 - Cisco Unity and the Cisco Unity server [8-23](#)
 - Example Administrator account against toll fraud [8-18](#)
- servers
 - restarting [B-3](#)
 - shutting down [B-3](#)
- Server Updates wizard
 - downloading latest [2-3](#)
- Server Updates wizard, running [5-10](#)
- service packs
 - downloading latest [2-3](#)
 - installing with Cisco Unity System Preparation Assistant [5-6](#)
- services, configuring Cisco Unity [8-7](#)
- setting
 - permissions with Cisco Unity Permissions wizard [7-4](#)
 - sa password for MSDE 2000 [5-9](#)
- setting up
 - Cisco Unity Administrator and Status Monitor to use SSL [8-15](#)
 - the Cisco PCA to use SSL [8-9](#)
- Setup program, Cisco Unity [8-3](#)
- shutting down
 - Cisco Unity server [B-3](#)
- software
 - configuring for D/120JCT-Euro voice card [A-7](#)
 - configuring for D/240PCI-T1 voice card [A-10](#)
 - configuring for PIMG units [A-12](#)
 - downloading for installation [2-2](#)
 - exiting Cisco Unity [B-1](#)
 - installing Cisco Unity [8-3](#)
 - installing Lotus Notes on Cisco Unity server [6-4](#)
 - installing optional [9-2](#)
 - registering Cisco Unity [5-4](#)
 - starting Cisco Unity [B-3](#)
- SQL Server 2000
 - installing Enterprise Manager for MSDE 2000 [5-9](#)
 - installing with Cisco Unity System Preparation Assistant [5-6](#)
 - moving databases and transaction logs [8-19](#)
- SSL
 - determining whether to use [8-2](#)
 - installing Microsoft Certificate Services component [8-3](#)
 - setting up Cisco Unity Administrator and Status Monitor to use [8-15](#)
 - setting up the Cisco PCA to use [8-9](#)
- starting
 - Cisco Unity software [B-3](#)
- Status Monitor, setting up to use SSL [8-15](#)
- switches and jumpers
 - D/240PCI-T1 [A-9](#)
 - D/41EPCI [A-2](#)
 - D/41JCT-LS and D/41JCT-Euro [A-4](#)

T

- TCP/IP properties, configuring [5-12](#)
- toll fraud, preventing [8-18](#)
- transaction logs
 - moving SQL Server 2000 or MSDE 2000 [8-19](#)

U

- UDDI Services, do not install [4-8](#)

Unity Messaging Repository conversation, enabling [8-22](#)
 universal PCI voice cards, slot placement [3-1](#)
 unknown PCI device error message [3-1](#)
 updates
 installing Windows, Internet Explorer, and SQL
 Server 2000 or MSDE 2000 [5-10](#)
 userva switch, adding to boot.ini for more than 96
 ports [4-12](#)
 utilities
 Windows 2000 Server installation, on disc from server
 manufacturer [4-9](#)
 Windows Server 2003 installation, on disc from server
 manufacturer [4-8](#)
 UTIM. *See* Cisco Unity Telephony Integration Manager

Windows components, installing with Cisco Unity System
 Preparation Assistant [5-6](#)
 Windows Explorer, changing folder settings in [5-10](#)
 Windows Server 2003
 installing using the PCD [4-4](#)
 UDDI Services, do not install [4-8](#)

V

verifying IP address and network connection [5-13](#)
 virus scanning
 disabling services [5-14](#)
 excluding directory in which Cisco Unity is
 installed [8-14](#)
 installing software [5-12](#)
 re-enabling services [8-22](#)
 voice cards
 D/120JCT-Euro [A-4](#)
 D/120JCT-LS [A-4](#)
 D/240PCI-T1 [A-8](#)
 D/41EPCI [A-1](#)
 D/41JCT-Euro [A-1](#)
 D/41JCT-LS [A-1](#)
 disabling Found New Hardware wizard for [5-11](#)
 installing [3-1](#)
 slot placement [3-1](#)

W

Windows 2000 Server
 installing using the PCD [4-4, 4-6](#)

